

Docket No.: 31869-201591
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Matsumura et al.

Application No.: Not Yet Assigned

Confirmation No.: N/A

Filed: Concurrently Herewith

Art Unit: N/A

For: METHOD OF RECONSTRUCTING A
SECRET, SHARED SECRET
RECONSTRUCTION APPARATUS, AND
SECRET RECONSTRUCTION SYSTEM

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	2003-067834	March 13, 2003

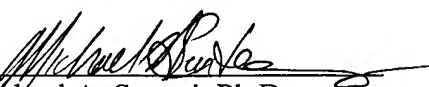
Application No.: Not Yet Assigned

Docket No.: 31869-201591

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 12, 2004

Respectfully submitted,

By 
Michael A. Sartori, Ph.D.

Registration No.: 41,289
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent For Applicant

MAS/trl
DC2-530685

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 3月13日

出願番号
Application Number: 特願2003-067834
[ST. 10/C]: [JP2003-067834]

出願人
Applicant(s): 沖電気工業株式会社

2003年11月21日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3096741

【書類名】 特許願

【整理番号】 MA001423

【提出日】 平成15年 3月13日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08

【発明者】

【住所又は居所】 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会
社内

【氏名】 松村 靖子

【発明者】

【住所又は居所】 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会
社内

【氏名】 中川 聡

【発明者】

【住所又は居所】 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会
社内

【氏名】 圓藤 康平

【特許出願人】

【識別番号】 000000295

【氏名又は名称】 沖電気工業株式会社

【代理人】

【識別番号】 100083840

【弁理士】

【氏名又は名称】 前田 実

【選任した代理人】

【識別番号】 100116964

【弁理士】

【氏名又は名称】 山形 洋一

【手数料の表示】

【予納台帳番号】 007205

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003703

【包括委任状番号】 0101807

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 秘密再構成方法、分散秘密再構成装置、及び秘密再構成システム

【特許請求の範囲】

【請求項 1】 秘密分散法を用いて、もとの秘密情報から n 個の第 1 の分散情報を生成し、上記 n 個の第 1 の分散情報を n 人 ($2 \leq n$) のメンバのそれぞれに配布している場合に、上記 n 人のメンバのうちの t ($2 \leq t \leq n$) 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法において、

上記集まった t 人のメンバのそれぞれが、秘密分散法を用いて、自分自身が保持する第 1 の分散情報から t 個の第 2 の分散情報を生成し、上記集まった t 人のメンバのそれぞれに配布する工程と、

上記集まった t 人のメンバのそれぞれが、自分自身が生成した第 2 の分散情報及び他のメンバから自分自身が受け取った ($t - 1$) 個の第 2 の分散情報を用いた分散計算により、上記もとの秘密情報を再構成するための t 個の中間計算結果を生成する工程と、

上記 t 個の中間計算結果から、上記もとの秘密情報を再構成する工程とを有することを特徴とする秘密再構成方法。

【請求項 2】 上記第 1 の分散情報は、上記 n 個の第 1 の分散情報をすべて加算した値が、上記もとの秘密情報となるような秘密分散法により得られたことを特徴とする請求項 1 に記載の秘密再構成方法。

【請求項 3】 上記第 2 の分散情報は、分散情報をすべて加算した値が第 1 の分散情報となるような秘密分散法により得られたことを特徴とする請求項 1 又は 2 のいずれかに記載の秘密再構成方法。

【請求項 4】 あるメンバが生成した上記中間計算結果は、上記あるメンバ自身が生成した第 2 の分散情報及び上記あるメンバ自身が受け取った ($t - 1$) 個の第 2 の分散情報をすべて加算することによって得られたことを特徴とする請求項 1 から 3 までのいずれかに記載の秘密再構成方法。

【請求項 5】 上記 n 個の第 1 の分散情報は、上記メンバのそれぞれを識別するためのメンバ ID を用いたしきい値秘密分散法により得られたことを特徴と

する請求項 1 に記載の秘密再構成方法。

【請求項 6】 上記第 2 の分散情報は、上記集まった t 人のメンバのそれぞれが持つ第 1 の分散情報を、メンバ ID を用いたしきい値秘密分散法、又は、分散情報をすべて加算することにより秘密再構成を行うことができる秘密分散法を用いて秘密分散することにより得られたことを特徴とする請求項 1 又は 5 のいずれかに記載の秘密再構成方法。

【請求項 7】 あるメンバが生成した上記中間計算結果は、上記あるメンバ自身が生成した第 2 の分散情報及び上記あるメンバ自身が受け取った $(t-1)$ 個の第 2 の分散情報を、上記あるメンバのメンバ ID に基づく係数を用いて線形結合計算することによって得られたことを特徴とする請求項 1、5、6 のいずれかに記載の秘密再構成方法。

【請求項 8】 上記集まった t 人のメンバに対して、互いに重複しない仮メンバ ID を生成して配布する工程をさらに有し、

上記もとの秘密情報を再構成するための上記中間計算結果を、上記仮メンバ ID を用いた分散計算により算出し、上記中間計算結果及び上記仮メンバ ID から、上記もとの秘密情報を再構成する

ことを特徴とする請求項 1、2、4、5、7 のいずれかに記載の秘密再構成方法。

【請求項 9】 秘密分散法により上記集まった t 人のメンバのメンバ ID から第 3 の分散情報を生成し、上記集まった t 人のメンバに配布する工程をさらに有することを特徴とする請求項 1、3、5、6、8 のいずれかに記載の秘密再構成方法。

【請求項 10】 秘密分散法を用いて、もとの秘密情報から n 個の第 1 の分散情報を生成し、上記 n 個の第 1 の分散情報を n 人 $(2 \leq n)$ のメンバのそれぞれに配布している場合に、上記 n 人のメンバのうちの t $(2 \leq t \leq n)$ 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法において分散計算を行う複数の分散秘密再構成装置の内の 1 台であって、上記各メンバが管理する分散秘密再構成装置において、

この分散秘密再構成装置が保有する第 1 の分散情報を秘密分散法を用いて分散

し、第2の分散情報として他の分散秘密再構成装置に配布する秘密分散手段と、
上記秘密分散手段からの出力と、上記他の分散秘密再構成装置から受け取った
第2の分散情報を用いて、上記もとの秘密情報を再構成するための中間計算結果
を、分散計算により算出する分散秘密再構成計算手段と、

上記分散秘密再構成計算手段の出力である上記中間計算結果を送信する送信手
段と

を有することを特徴とする分散秘密再構成装置。

【請求項11】 秘密分散法を用いて、もとの秘密情報から n 個の第1の分散
情報を生成し、上記 n 個の第1の分散情報を n 人 ($2 \leq n$) のメンバのそれぞ
れに配布している場合に、上記 n 人のメンバのうちの t ($2 \leq t \leq n$) 人のメン
バが集まって、上記もとの秘密情報を再構成する秘密再構成方法において分散計
算を行う複数の分散秘密再構成装置の内の1台であって、上記各メンバが管理す
る分散秘密再構成装置において、

この分散秘密再構成装置が保有する第1の分散情報を秘密分散法を用いて分散
し、第2の分散情報として他の分散秘密再構成装置に配布する秘密分散手段と、

上記秘密分散手段からの出力と、上記他の分散秘密再構成装置から受け取った
第2の分散情報を用いて、上記もとの秘密情報を再構成するための中間計算結果
を、分散計算により算出する分散秘密再構成計算手段と、

上記分散秘密再構成計算手段からの出力と、上記他の分散秘密再構成装置の出
力を受け取り、それらの出力から、上記もと秘密情報を再構成する秘密再構成手
段と

を有することを特徴とする分散秘密再構成装置。

【請求項12】 上記分散秘密再構成計算手段からの出力と、他の分散秘密
再構成装置のからの出力を受け取り、それらの出力から、もと秘密情報を再構成
する秘密再構成手段をさらに有することを特徴とする請求項10に記載の分散秘
密再構成装置。

【請求項13】 上記秘密分散手段は、分散情報をすべて加算した値がもと
の秘密情報となるような秘密分散法を用いることを特徴とする請求項10から1
2までのいずれかに記載の分散秘密再構成装置。

【請求項 14】 上記分散秘密再構成計算手段は、上記秘密分散手段からの出力と、他の分散再構成装置から受け取った第2の分散情報をすべて加算する加算手段を含むことを特徴とする請求項10から13までのいずれかに記載の分散秘密再構成装置。

【請求項 15】 上記秘密分散手段は、メンバIDを用いたしきい値秘密分散法を用いることを特徴とする請求項10、11、12、14のいずれかに記載の分散秘密再構成装置。

【請求項 16】 上記分散秘密再構成計算手段は、上記秘密分散手段からの出力と、秘密通信路を通して他の分散秘密再構成装置から受け取った第2の分散情報を、メンバIDから計算される係数を用いて線形結合計算をする線形結合計算手段を含むことを特徴とする請求項10、11、12、13、15のいずれかに記載の分散秘密再構成装置。

【請求項 17】 上記秘密分散手段は、この分散秘密再構成装置に配布された仮メンバIDを用いたしきい値秘密分散法を用いることを特徴とする請求項10、11、12、14、16のいずれかに記載の分散秘密再構成装置。

【請求項 18】 上記秘密分散手段は、この分散秘密再構成装置が保有するメンバIDを秘密分散法を用いて分散し、第3の分散情報として他の分散秘密再構成装置に配布し、

上記分散秘密再構成計算手段は、上記秘密分散手段から出力される第2及び第3の分散情報と、他の分散秘密再構成装置から受け取った第2及び第3の分散情報を用いて、秘密再構成の中間計算結果を、分散計算により算出する

ことを特徴とする請求項10、11、12、13、17のいずれかに記載の分散秘密再構成装置。

【請求項 19】 上記分散秘密再構成計算手段は、

上記秘密分散手段から出力される第2及び第3の分散情報と、他の分散秘密再構成装置から受け取った第2及び第3の分散情報を用いて、第2の分散情報に対する、第3の分散情報から計算される係数を分散計算した結果と、その各第2の分散情報との分散乗算を行う項計算手段と、

上記項計算手段の出力を、すべて足し合わせる加算手段と

を含むことを特徴とする請求項 10、11、12、13、17、18 のいずれかに記載の分散秘密再構成装置。

【請求項 20】 上記項計算手段は、
異なる第 3 の分散情報同士の差分をとる差分計算手段と、
上記差分計算手段の出力を分散乗算する第 1 の多項分散乗算手段と、
上記第 1 の多項分散乗算手段の出力の逆元を分散計算する分散逆元計算手段と、
第 3 の分散情報を分散乗算する第 2 の多項分散乗算手段と、
上記分散逆元計算手段の出力と、第 2 の多項分散乗算手段の出力と、対応する第 2 の分散情報とを分散乗算する第 3 の多項分散乗算手段と、
を含むことを特徴とする請求項 10、11、12、13、17、18、19 のいずれかに記載の分散秘密再構成装置。

【請求項 21】 上記第 1、第 2、及び第 3 の多項分散乗算手段はそれぞれ、分散乗算する値の個数よりも 1 小さい個数の、2 つの値を分散乗算する二項分散乗算手段を含むことを特徴とする請求項 10、11、12、13、17、18、19、20 のいずれかに記載の分散秘密再構成装置。

【請求項 22】 上記二項分散乗算手段はそれぞれ、
入力される 2 つの入力を掛け合わせる乗算手段と、
上記乗算手段の出力を、仮メンバ ID を用いたしきい値秘密分散法で分散し、
第 4 の分散情報として他の分散秘密再構成装置に対して秘密通信路を通して配布する第 2 の秘密分散手段と、

上記第 2 の秘密分散手段からの出力と、他の分散秘密再構成装置から秘密通信路を通して受け取った第 4 の分散情報を、仮メンバ ID から計算される係数を用いて線形結合計算をする線形結合計算手段と、

を含むことを特徴とする請求項 10、11、12、17、18、19、20、21 のいずれかに記載の分散秘密再構成装置。

【請求項 23】 上記二項分散乗算手段はそれぞれ、
入力される 2 つの入力を掛け合わせ、さらに仮メンバ ID から計算される係数を掛け合わせる第 1 の乗算手段と、

入力される第1の入力と、他の分散秘密再構成装置の対応する項分散乗算手段への第2の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第1の通信計算手段と、

入力される第2の入力と、他の分散秘密再構成装置の対応する項分散乗算手段への第1の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第2の通信計算手段と、

第1の通信計算手段の出力と第2の計算手段の出力を足し合わせる加算手段と、

上記加算手段の出力に、仮メンバーIDから計算される係数を掛け合わせる第2の乗算手段と、

上記第1の乗算手段の結果と上記第2の乗算手段の結果とをすべて足し合わせる第2の加算手段と、

を含むことを特徴とする請求項10、11、12、17、18、19、20、21のいずれかに記載の分散秘密再構成装置。

【請求項24】 上記二項分散乗算手段はそれぞれ、

入力される2つの入力を掛け合わせる第1の乗算手段と、

入力される第1の入力と、他の分散秘密再構成装置の対応する二項分散乗算手段への第2の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第1の通信計算手段と、

入力される第2の入力と、他の分散秘密再構成装置の対応する二項分散乗算手段への第1の入力との乗算結果を、秘密通信路を通して紛失通信を行うことにより計算する第2の通信計算手段と、

第1の通信計算手段の出力と第2の計算手段の出力を足し合わせる加算手段と、

上記第1の乗算手段の結果と上記加算手段の結果とをすべて足し合わせる第2の加算手段と、

を含むことを特徴とする請求項10、11、12、13、18、19、20、21のいずれかに記載の分散秘密再構成装置。

【請求項25】 上記分散逆元計算手段は、



演算に用いる有限体の大きさから計算される第 1 の個数の、“上記請求項 2 2、2 3 又は 2 4 のいずれかに記載の二項分散乗算手段と同じ構成を持つ二項分散乗算手段と、

分散乗算する値の個数が、演算に用いる有限体の大きさから計算される第 2 の個数である上記請求項 2 1 に記載の第 1、第 2、及び第 3 の多項分散乗算手段と同じ構成を持つ多項分散乗算手段と

を含むことを特徴とする請求項 1 0、1 1、1 2、1 3、1 7、1 8、1 9、2 0、2 1、2 2、2 3、2 4 のいずれかに記載の分散秘密再構成装置。

【請求項 2 6】 上記分散逆元計算手段は、

乱数を生成する乱数生成手段と、

入力される値とその乱数生成手段の出力とを入力とする、上記請求項 2 2 又は請求項 2 3 のいずれかに記載の二項分散乗算手段と同じ構成を持つ第 2 の二項分散乗算手段と、

上記第 2 の二項分散乗算手段からの出力と、秘密通信路を通して受け取ったほかの分散秘密再構成装置の対応する第 2 の二項分散乗算手段の出力を、仮メンバー ID から計算される係数を用いて線形結合計算をする線形結合計算手段と、

上記線形結合計算手段の出力の有限体上の演算における逆元を計算する逆元計算手段と、

上記逆元計算手段の結果を分散し、第 5 の分散情報として他の分散秘密再構成装置に対して秘密通信路を通して配布する秘密分散手段と、

上記秘密分散手段における第 5 の分散情報と、その乱数生成手段からの出力とを入力とする、上記請求項 2 2 又は請求項 2 3 のいずれかに記載の二項分散乗算手段と同じ構成を持つ第 3 の二項分散乗算手段と、

を含むことを特徴とする請求項 1 0、1 1、1 2、1 7、1 8、1 9、2 0、2 1、2 2、2 3 のいずれかに記載の分散秘密再構成装置。

【請求項 2 7】 上記分散逆元計算手段は、

乱数を生成する乱数生成手段と、

入力される値とその乱数生成手段の出力とを入力とする、上記請求項 2 4 に記載の二項分散乗算手段と同じ構成を持つ第 2 の二項分散乗算手段と、

上記第2の二項分散乗算手段からの出力と、秘密通信路を通して受け取ったほかの分散秘密再構成装置の対応する第2の二項分散乗算手段の出力をすべて足し合わせる加算手段と、

上記線形結合計算手段の出力の有限体上の演算における逆元を計算する逆元計算手段と、

上記逆元計算手段の結果を分散し、第5の分散情報として他の分散秘密再構成装置に対して秘密通信路を通して配布する秘密分散手段と、

上記秘密分散手段における第5の分散情報と、その乱数生成手段からの出力とを入力とする、上記請求項24に記載の二項分散乗算手段と同じ構成を持つ第3の二項分散乗算手段と、

を含むことを特徴とする請求項10、11、12、13、18、19、20、21、24のいずれかに記載の分散秘密再構成装置。

【請求項28】 上記分散逆元計算手段は、

乱数を生成する乱数生成手段と、

入力される値とその乱数生成手段の出力とを入力とする、上記請求項22、23又は24のいずれかに記載の二項分散乗算手段と同じ構成を持つ第4の二項分散乗算手段と、

上記第4の二項分散乗算手段の計算結果を、上記請求項26又は27に記載の分散秘密再構成装置と同じ構成を持つ分散秘密再構成装置へ送信する送信手段と、

上記請求項26又は27に記載の分散秘密再構成装置と同じ構成を持つ分散秘密再構成装置から、上記第5の分散情報を受信する受信手段と、

上記受信した第5の分散情報と、その乱数生成手段からの出力とを入力とする、上記請求項22、23又は24のいずれかに記載の二項分散乗算手段と同じ構成を持つ第5の二項分散乗算手段と

を含むことを特徴とする、請求項10、11、12、13、17、18、19、20、21、22、23、24のいずれかに記載の分散秘密再構成装置。

【請求項29】 秘密分散法を用いて、もとの秘密情報から n 個の第1の分散情報を生成し、上記 n 個の第1の分散情報を n 人($2 \leq n$)のメンバーのそれぞれ

れに配布している場合に、上記 n 人のメンバのうち t ($2 \leq t \leq n$) 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項 10、11、12 のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

上記分散秘密再構成装置の出力から、上記もとの秘密情報を再構成する秘密再構成装置と

を有することを特徴とする秘密再構成システム。

【請求項 30】 秘密分散法を用いて、もとの秘密情報から n 個の第 1 の分散情報を生成し、上記 n 個の第 1 の分散情報を n 人 ($2 \leq n$) のメンバのそれぞれに配布している場合に、上記 n 人のメンバのうち t ($2 \leq t \leq n$) 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項 10 から 28 までのいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置を有し、

上記複数台の分散秘密再構成装置の内の少なくとも 1 台以上は、上記分散秘密再構成手段からの出力と、他の分散秘密再構成装置の出力を受け取り、それらの出力から、上記もとの秘密情報を再構成する秘密再構成手段を有する

ことを特徴とする秘密再構成システム。

【請求項 31】 秘密分散法を用いて、もとの秘密情報から n 個の第 1 の分散情報を生成し、上記 n 個の第 1 の分散情報を n 人 ($2 \leq n$) のメンバのそれぞれに配布している場合に、上記 n 人のメンバのうち t ($2 \leq t \leq n$) 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項 10、11、12、13、14、16、18、19、20、21、24、25、27、28 のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

分散情報をすべて加算した値がもとの秘密情報となるような秘密分散法の再構成を用いて、上記複数台の分散情報再構成装置の出力から、上記もとの秘密情報

を再構成する秘密再構成装置と

を有することを特徴とする秘密再構成システム。

【請求項 3 2】 秘密分散法を用いて、もとの秘密情報から n 個の第 1 の分散情報を生成し、上記 n 個の第 1 の分散情報を n 人 ($2 \leq n$) のメンバのそれぞれに配布している場合に、上記 n 人のメンバのうち t ($2 \leq t \leq n$) 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

上記請求項 1 0、1 1、1 2、1 4、1 5、1 6 のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

メンバ ID を用いたしきい値秘密分散法の再構成方法を用いて、上記複数台の分散秘密再構成装置の出力から、上記もとの秘密情報を再構成する秘密再構成装置と、

を有することを特徴とする秘密再構成システム。

【請求項 3 3】 秘密分散法を用いて、もとの秘密情報から n 個の第 1 の分散情報を生成し、上記 n 個の第 1 の分散情報を n 人 ($2 \leq n$) のメンバのそれぞれに配布している場合に、上記 n 人のメンバのうち t ($2 \leq t \leq n$) 人のメンバが集まって、上記もとの秘密情報を再構成する秘密再構成方法を実施する秘密再構成システムにおいて、

集まったメンバが管理する分散秘密再構成装置に対して、互いに重複しない仮メンバ ID を生成し、各分散秘密再構成装置に配布して、各分散秘密再構成装置にすべての仮メンバ ID を公開する仮メンバ ID 生成手段と、

上記請求項 1 0、1 1、1 2、1 4、1 6、1 7、1 8、1 9、2 0、2 1、2 2、2 3、2 5、2 6、2 8 のいずれかに記載の分散秘密再構成装置と同じ構成を持つ複数台の分散秘密再構成装置と、

仮メンバ ID を用いたしきい値秘密分散法の再構成を用いて、上記複数台の分散秘密再構成装置の出力から、上記もとの秘密情報を再構成する秘密再構成装置と、

を有することを特徴とする秘密再構成システム。

【請求項 3 4】 上記第 1 の分散情報は、分散情報をすべて加算した値がも

との情報となるような秘密分散法を用いることを特徴とする請求項 29、30、31、32、33 のいずれかに記載の秘密再構成システム。

【請求項 35】 上記第 1 の分散情報はメンバ ID を用いたしきい値秘密分散法を用いることを特徴とする請求項 29、30、31、32、33 のいずれかに記載の秘密再構成システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、秘密分散法により各メンバに分散された分散情報からもとの秘密情報を再構成する秘密再構成方法、この秘密再構成方法を実施する際に使用される分散秘密再構成装置、及びこの分散秘密再構成装置を含む秘密再構成システムに関するものである。

【0002】

【従来の技術】

情報の秘匿のための暗号化に用いる秘密鍵や認証を行うための秘密などの重要な秘密情報を保管する場合、その秘密情報の紛失や破壊の心配と、その秘密情報の盗難の心配がある。秘密情報を紛失や破壊により失ってしまうことへの対策としては、その秘密情報のコピーを作成し保管することが考えられるが、秘密情報のコピーが増えることにより、その秘密情報の盗難の危険性が増してしまう。この問題を解決する方法として、秘密分散法がある。秘密分散法を実施するシステムにおいては、秘密分散装置（演算装置）が、もとの秘密情報を複数の分散情報に分散（符号化）させ、関係者である各メンバ（演算記憶装置）にそれらの複数の分散情報をそれぞれ配布しておき、もとの秘密情報を得る必要がある場合には、秘密再構成装置（演算装置）が、必要なメンバから分散情報を集め、もとの秘密情報の再構成（復元）を行なう。

【0003】

秘密分散法の一つに、Shamir 法（シャミア法：Shamir's method）と呼ばれる (k, n) しきい値秘密分散法がある（例えば、非特許文献 1 参照）。非特許文献 1 に記述された (k, n) しきい値秘密分散法においては、秘密情報を

n (n は 2 以上の整数) 個の分散情報に符号化し、 k (k は n 以下の整数) 個以上の分散情報が集まれば、もとの秘密情報を復元することができるが、 $k-1$ 個以下の分散情報を集めても、もとの秘密情報を全く知ることができないという性質を、多項式補間を用いることにより実現している。

【0004】

具体的には、次式 (1) に示されるような $k-1$ 次多項式 $f(x)$ を用いてもとの秘密情報を分散する。

$$f(x) = S + R_1 x + R_2 x^2 + \dots + R_{k-1} x^{k-1} \quad \dots (1)$$

ここで、 S は、もとの秘密情報であり、 R_1, R_2, \dots, R_{k-1} は、分配者が決める乱数である。

【0005】

分散情報が配布される n 人の各メンバにメンバ ID として、 m_1, m_2, \dots, m_n が付与されている場合に、メンバ ID m_j ($j = 1, 2, \dots, n$) に対する分散情報 X_{m_j} は、上記式 (1) を用いて、次式 (2) のように計算できる。

$$X_{m_j}$$

$$= f(m_j)$$

$$= S + R_1 m_j + R_2 (m_j)^2 + \dots + R_{k-1} (m_j)^{k-1} \quad \dots (2)$$

【0006】

図 1 は、 (k, n) しきい値秘密分散法に基づく秘密分散を実施する秘密分散計算部 101 の動作を説明するための図である。図 1 に示されるように、秘密分散計算部 101 は、もとの秘密情報 S 及びこの秘密情報の分散情報が配布されるメンバ全員のメンバ ID m_j ($j = 1, 2, \dots, n$) を受け取り、もとの秘密情報 S に基づいて上記式 (1) の多項式 $f(x)$ を生成し、その多項式 $f(x)$ 及びメンバ ID m_j に基づいて、各メンバ ID m_j に対応する分散情報 X_{m_j} を、上記式 (2) を用いて生成して出力する。出力した各分散情報 X_{m_j} はそれぞれ、対応するメンバ ID を持つメンバに秘密裏に配布する。

【0007】

各メンバに配布した分散情報からもとの秘密情報 S を再構成する際には、分散情報が分配された n 人のメンバのうち t 人 ($k \leq t \leq n$) のメンバを集め、集め

られた t 人のメンバのメンバ ID m'_1, m'_2, \dots, m'_t と分散情報 $Xm'_1, Xm'_2, \dots, Xm'_t$ を持ち寄り、次式 (3) 及び (4) を用いて、もとの秘密情報 S を計算する。

【数 1】

$$S = r m'_1 X m'_1 + r m'_2 X m'_2 + \dots + r m'_t X m'_t \\ = \sum_{j=1}^t r m'_j X m'_j \quad (3)$$

$$r m'_j = (m'_1 \times m'_2 \times \dots \times m'_t / m'_j) \\ \div ((m'_1 - m'_j) \times (m'_2 - m'_j) \times \dots \times (m'_{j-1} - m'_j) \times (m'_{j+1} - m'_j) \times \dots \times (m'_t - m'_j)) \\ = \prod_{\substack{i=1 \\ i \neq j}}^t m'_i / (m'_i - m'_j) \quad (4)$$

【0008】

【非特許文献 1】

岡本龍明他、「現代暗号」(産業図書)、第 214-216 ページ及び第 227-236 ページ

【0009】

【発明が解決しようとする課題】

しかしながら、上記した方法により、もとの秘密情報 S の再構成を行う場合には、集まったメンバのメンバ ID m'_1, m'_2, \dots, m'_t や、そのメンバの分散情報 $Xm'_1, Xm'_2, \dots, Xm'_t$ を公開しなければ、もとの秘密情報 S を計算することができない。また、秘密再構成を行うセンターのようなものがあった場合であっても、集まったメンバのメンバ ID m'_1, m'_2, \dots, m'_t や分散情報 $Xm'_1, Xm'_2, \dots, Xm'_t$ をセンターに対して申告しなければ、もとの秘密情報 S を計算することができない。すなわち、集まったメンバを匿名にしたまま秘密情報 S を計算することはできなかった。

【0010】

また、秘密再構成を行うセンターのようなものがない場合には、集まったメンバに、自分の持つ分散情報 $Xm'_1, Xm'_2, \dots, Xm'_t$ を公開しなければ、

もとの秘密情報Sを求めることができない。すなわち、一旦、もとの秘密情報の再構成を行ってしまうと、メンバに配布した分散情報が露呈してしまうので、その露呈した分散情報を再利用することができず、もう一度秘密情報の分散処理を行う必要があった。

【0011】

そこで、本発明は上記したような従来技術の課題を解決するためになされたものであり、その目的は、各メンバを匿名にしたまま、各メンバの保有する分散情報を公開せずに、もとの秘密情報の再構成を行うことができる秘密再構成方法、この秘密再構成方法を実施する際に使用する分散秘密再構成装置、及びこの分散秘密再構成装置を含む秘密再構成システムを提供することにある。

【0012】

【課題を解決するための手段】

本発明の秘密再構成方法は、秘密分散法を用いてある秘密情報から n 個の第1の分散情報を生成し、前記 n 個の第1の分散情報を n 人 ($2 \leq n$) からなるグループの各メンバにそれぞれ配布している場合に、上記 n 人のメンバのうちの t ($2 \leq t \leq n$) 人のメンバが集まって、もとの秘密情報を再構成する方法である。この秘密再構成方法は、集まった t 人のメンバのそれぞれが、秘密分散法を用いて自身が保持する第1の分散情報から t 個の第2の分散情報を生成し、集まった t 人のメンバのそれぞれに配布する工程と、集まった t 人のメンバのそれぞれが、自身が生成した第2の分散情報及び入力された $(t-1)$ 個の第2の分散情報を用いた分散計算により、もとの秘密情報を再構成するための t 個の中間計算結果を生成する工程と、集まった t 人のメンバのそれぞれが生成した t 個の中間計算結果からもとの秘密情報を再構成する工程とを有する。

【0013】

【発明の実施の形態】

＜第1の実施形態＞

[第1の実施形態の概要]

本発明の第1の実施形態においては、もとの秘密情報Sを再構成する際に、もとの秘密情報Sを再構成するために集まったメンバ（演算記憶装置）が保有する

分散情報を用いてマルチパーティ・プロトコルを実行することにより、各メンバーが保有する分散情報を公開せずに、もとの秘密情報 S の再構成を行う。なお、第 1 の実施形態に係る秘密再構成方法は、秘密再構成システムにより実施される。第 1 の実施形態に係る秘密再構成システムは、各メンバー（演算記憶装置）である分散秘密再構成装置（後述する分散秘密再構成計算部 301）と、メンバーのいずれかに又はメンバーとは別のセンターに備えられた演算装置（後述する秘密再構成計算部 302）とを主要な構成としている。

【0014】

[マルチパーティ・プロトコルの説明]

次に、マルチパーティ・プロトコルの説明をする。マルチパーティ・プロトコルとは、ある関数への入力値を公開せずに、その関数の計算を集まったメンバーで協力して行う方式であり、「分散計算」とも呼ばれる（例えば、前述した非特許文献 1 参照）。マルチパーティ・プロトコルには、大きく分けて 2 つの方式がある。第 1 の方式は、計算するために集まったメンバーのうち、どの 2 人のメンバー間にも、その 2 人のメンバー以外には通信内容を秘密とすることができる秘密通信路が確立されていることを前提とする方式である。第 2 方式は、計算するために集まったメンバー間の通信には、前述した秘密通信路による通信方法に加え、紛失通信と呼ばれる通信手法を用いる方式である。前述した非特許文献 1 には、マルチパーティ・プロトコルの第 2 方式における、バイナリ計算（NOT と AND の計算）の場合の説明が記載されている。また、マルチパーティ・プロトコルの第 2 方式の詳細は、後述する第 4 の実施形態において説明する。

【0015】

ここでは、有限体要素の計算（加算と乗算の計算）を用いるマルチパーティ・プロトコルの第 1 方式について説明する。マルチパーティ・プロトコルを実行するメンバーが t 人いる場合を想定する。メンバーのそれぞれが、メンバー ID として m_j ($j = 1, 2, \dots, t$) と、そのメンバー固有の秘密情報 X_{m_j} ($j = 1, 2, \dots, t$) を所有しており、次式 (5) に示される関数値 Y をマルチパーティ・プロトコルで計算する場合を考える。

$$Y = f(X_{m_1}, X_{m_2}, \dots, X_{m_t}) \quad \dots (5)$$

ここで、各メンバのメンバIDである m_j 及び秘密情報 Xm_j ($j = 1, 2, \dots, t$) は、有限体 $GF(q)$ (q は素数又は素数のべき乗) 上の値であるものとする。また、上記式(5)の関数 f における演算は、有限体 $GF(q)$ 上の演算であるものとし、したがって、得られる関数値 Y も、有限体 $GF(q)$ 上の値となる。

【0016】

各メンバ固有の秘密情報 Xm_j ($j = 1, 2, \dots, t$) を、他のメンバに公開しないまま、関数値 Y を計算するために、マルチパーティ・プロトコルでは、まず、各メンバ固有の秘密情報 Xm_j ($j = 1, 2, \dots, t$) を、 (k, t) しい値秘密分散法を用いて秘密分散し、各メンバに配布する。メンバIDが m_j であるメンバの秘密情報が Xm_j であるとする、このメンバは、次式(6)の $k-1$ ($k \leq t$) 次多項式 $f_{m_j}(x)$ を作る。

【数2】

$$f_{m_j}(x) = Xm_j + R_{m_j,1}x + R_{m_j,2}x^2 + \dots + R_{m_j,k-1}x^{k-1} \quad (6)$$

ここで、 $R_{m_j,1}, R_{m_j,2}, \dots, R_{m_j,k-1}$ は、有限体 $GF(q)$ 上の値から選ばれた $k-1$ 個の乱数である。

【0017】

秘密情報 Xm_j を秘密分散法により分散し、メンバIDが m_p ($p = 1, 2, \dots, t$) であるメンバに対して配布される分散情報を $Xm_{j,p}$ と表記する場合には、分散情報 $Xm_{j,p}$ は、上記式(6)を用いて、次式(7)のよう計算できる。

【数3】

$$\begin{aligned} Xm_{j,p} &= f_{m_j}(m_p) \\ &= Xm_j + R_{m_j,1}(m_p) + R_{m_j,2}(m_p)^2 + \dots + R_{m_j,k-1}(m_p)^{k-1} \end{aligned} \quad (7)$$

なお、分散情報 $Xm_{j,p}$ は、メンバIDが m_p ($p = 1, 2, \dots, t$) であるメンバ以外には秘密となるよう、秘密通信路を用いて、メンバIDが m_p ($p =$

1, 2, ..., t) であるメンバに配布する。

【0018】

上記式(6)及び(7)における足し算及び掛け算は、有限体GF(q)上における加算及び乗算であるものとする。したがって、得られる分散情報 X_{m_j} , p ($j=1, 2, \dots, t$; $p=1, 2, \dots, t$)は、有限体GF(q)上の値である。なお、以下の説明においては、断りが無い限り、演算は有限体GF(q)上で行われるものとする。

【0019】

以上の処理によって、各メンバは、他の各メンバの秘密情報 X_{m_j} の分散情報 $X_{m_j, p}$ を持っている状態になる。メンバIDが m_j であるメンバは、他のメンバから配布された分散情報(及び自分自身の秘密情報の分散情報) $X_{m_1, j}$, $X_{m_2, j}$, ..., $X_{m_t, j}$ のt個の分散情報を持っていることになる。

【0020】

ここで、マルチパーティ・プロトコルにおける分散加算(足し算計算)を行う。上記式(5)の関数が、例えば、次式(8)に示されるような、ある2つの入力 X_{m_A} 及び X_{m_B} の足し算となっている場合、

$$Y = f(X_{m_1}, X_{m_2}, \dots, X_{m_t}) = X_{m_A} + X_{m_B} \quad \dots (8)$$

マルチパーティ・プロトコルでは、各メンバは、入力 X_{m_A} 及び X_{m_B} の分散情報同士の足し算を行うことで、計算結果Yの分散情報 Y_{m_j} ($j=1, 2, \dots, t$)を得ることができる。例えば、メンバIDが m_j であるメンバは、入力 X_{m_A} 及び X_{m_B} の分散情報として、それぞれ $X_{m_A, j}$ 及び $X_{m_B, j}$ を持っているので、次式(9)のような計算を行い、計算結果Yの分散情報 Y_{m_j} を得る。

$$Y_{m_j} = X_{m_A, j} + X_{m_B, j} \quad \dots (9)$$

【0021】

次に、マルチパーティ・プロトコルにおける分散乗算(掛け算計算)を説明する。上記式(5)の関数が、例えば、次式(10)のような、ある2つの入力 X_{m_A} 及び X_{m_B} の掛け算となっている場合、

$$Y = f(X_{m_1}, X_{m_2}, \dots, X_{m_t}) = X_{m_A} \times X_{m_B} \quad \dots (10)$$

マルチパーティ・プロトコルでは、各メンバは、次のようなステップS101～

S103の処理を行う。ステップS101においては、入力 X_{m_A} 及び X_{m_B} の分散情報同士の掛け算を行い、ステップS102においては、その掛け算結果をさらに、他のメンバに秘密分散して配布し、ステップS103においては、受け取った側でそれらの再構成を行うことで、計算結果 Y の分散情報 Y_{m_j} ($j = 1, 2, \dots, t$)を得ることができる。ただし、第1方式における、マルチパーティ・プロトコルの分散乗算では、秘密分散のしきい値 k は、次式(11)となっている必要がある。

$$k \leq (t+1)/2 \quad \dots (11)$$

ここで、上記式(11)の演算は、有限体 $GF(q)$ 上の演算ではなく、通常の実数、整数演算である。

【0022】

具体的に説明すると、例えば、メンバIDが m_j であるメンバは、入力 X_{m_A} 及び X_{m_B} の分散情報として、それぞれ $X_{m_A, j}$ 及び $X_{m_B, j}$ を持っているので、まず、次式(12)のような計算を行い、途中計算結果 Y'_{m_j} を得る(上記ステップS101)。

$$Y'_{m_j} = X_{m_A, j} \times X_{m_B, j} \quad \dots (12)$$

【0023】

次に、この途中計算結果 Y'_{m_j} を次式(13)のような多項式で秘密分散を行う(上記ステップS102)。

【数4】

$$f'_{m_j}(x) = Y'_{m_j} + R'_{m_j, 1} x + R'_{m_j, 2} x^2 + \dots + R'_{m_j, k-1} x^{k-1} \quad (13)$$

ここで、 $R'_{m_j, 1}, R'_{m_j, 2}, \dots, R'_{m_j, k-1}$ は、乱数として有限体 $GF(q)$ 上の値を $k-1$ 個選ぶことによって得られる。

【0024】

次に、メンバIDが m_p ($p = 1, 2, \dots, t$)であるメンバに対して配布する自分の途中計算結果 Y'_{m_j} の分散情報 $Y'_{m_j, p}$ を、上記式(13)を用いて、次式(14)のように計算する。

【数5】

$$\begin{aligned}
 Y'm_{j,p} &= f'm_j(m_p) \\
 &= Y'm_j + R'm_{j,1}(m_p) + R'm_{j,2}(m_p)^2 + \cdots + R'm_{j,k-1}(m_p)^{k-1} \quad (14)
 \end{aligned}$$

なお、メンバIDが m_p ($p = 1, 2, \dots, t$)であるメンバ以外には秘密となるよう、秘密通信路を用いてメンバIDが m_p ($p = 1, 2, \dots, t$)であるメンバに配布する。上記式(14)のような計算で分散した結果、メンバIDが m_j であるメンバは、 $Y'm_{1,j}, Y'm_{2,j}, \dots, Y'm_{t,j}$ の t 個の分散情報を受け取る。

【0025】

メンバIDが m_j であるメンバは、これら分散情報 $Y'm_{1,j}, Y'm_{2,j}, \dots, Y'm_{t,j}$ から、掛け算結果の分散情報 Ym_j を次式(15)及び(16)のように計算する。

【数6】

$$\begin{aligned}
 Ym_j &= r m_1 Y'm_{1,j} + r m_2 Y'm_{2,j} + \cdots + r m_t Y'm_{t,j} \\
 &= \sum_{i=1}^t r m_i Y'm_{i,j} \quad (15)
 \end{aligned}$$

$$\begin{aligned}
 r m_j &= (m_1 \times m_2 \times \cdots \times m_t / m_j) \\
 &\quad / ((m_1 - m_j) \times (m_2 - m_j) \times \cdots \times (m_{j-1} - m_j) \times (m_{j+1} - m_j) \times \cdots \times (m_t - m_j)) \\
 &= \prod_{\substack{i=1 \\ i \neq j}}^t m_i / (m_i - m_j) \quad (16)
 \end{aligned}$$

この計算は、秘密情報の再構成時の計算(前述した式(3))と同様のものである(上記ステップS103)。

【0026】

上記のように、マルチパーティ・プロトコルを用いれば、各メンバ同士が秘密通信を行って計算処理をすることにより、入力値を公開せずに、与えられた関数の計算を行うことができる。

【0027】

[第1の実施形態の構成]

第1の実施形態は、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報Sを、(k, n) しきい値秘密分散法ではなく、単純な加減算による秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。すなわち、図2に示されるように、秘密分散法を用いてもとの秘密情報Sから分散情報を生成し、生成された分散情報が各メンバに配布されている場合を前提とする。図2は、秘密分散法を実施する秘密分散計算部201の動作を説明するための図である。秘密分散計算部201は、前述した図1の秘密分散計算部101とは動作が異なり、次のような計算を行う。ここで、秘密分散計算部201へ入力されるもとの秘密情報をS（これは、有限体GF(q)上の要素とする）とし、分散情報が配布されるメンバがn人であるとする。秘密分散計算部201は、まず、有限体GF(q)から乱数をn-1個選ぶ。それらの乱数 X_1, X_2, \dots, X_{n-1} から、次式(17)を満たす X_n を求める。

$$X_n = S - (X_1 + X_2 + \dots + X_{n-1}) \quad \dots (17)$$

【0028】

秘密分散計算部201は、上記式(17)により得られた値 X_1, X_2, \dots, X_n を出力し、各メンバに重複しないように配布する。値 X_1, X_2, \dots, X_n のうち、いくつかは等しい値であってもよい。上記式(17)の計算は、有限体GF(q)上で行われる。以降の説明においては、断りがない限り、演算は、有限体GF(q)上で行われるものとする。

【0029】

上記したような秘密分散法によりもとの秘密情報Sを分散した場合には、分散情報が配布されたメンバ全員（すなわちn人）が集まらない限り、もとの秘密情報Sを再構成することができない。もとの秘密情報Sは、次式(18)を計算することにより、再構成できる。

$$S = X_1 + X_2 + \dots + X_n \quad \dots (18)$$

【0030】

上記したような秘密分散法を、「加算秘密分散法」と呼ぶこととする。第1の実施形態は、上記した加算秘密分散法により秘密分散された分散情報を各メンバ



に配布し、各メンバが分散情報を所有している状態を前提とする。もとの秘密情報 S を再構成させたいときに、集まったメンバ (n 人) が分散情報を持ち寄り、上記式 (18) を用いてもとの秘密情報 S を再構成することができるが、第 1 の実施形態に係る秘密再構成方法においては、この再構成時の計算を、マルチパーティ・プロトコルで分散計算することにより、集まった各メンバの分散情報を公開せずに、もとの秘密情報 S を再構成する。

【0031】

第 1 の実施形態においては、複数のメンバからなるあるグループで、前述の秘密分散法 (上記式 (17) による方法) を用いてもとの秘密情報 S から生成された分散情報が、各メンバに秘密裏に配布されている状態を前提とする。このグループには n 人のメンバがいるものとし、もとの秘密情報 S から生成され、各メンバに配布された分散情報を X_j ($j = 1, 2, \dots, n$) とする。

【0032】

第 1 の実施形態において、もとの秘密情報 S を再構成する際に、メンバ全員 (すなわち、 n 人のメンバ) が集まり、各メンバの持つ分散情報を持ち寄る。また、メンバのうち、どの 2 人のメンバ間にも、その 2 人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されているものとする。図 3 は、第 1 の実施形態において各メンバ間の通信に用いる秘密通信路 303 を示す図である。図 3 において、四角形で示されるブロックは集まったメンバを示し、 $m'_1, m'_2, \dots, m'_j, \dots, m'_t$ は、メンバ ID を示し、両方向の矢印は、それぞれ対応するメンバ以外には通信内容を秘密とする秘密通信路 303 を示している。

【0033】

次に、図 4 を用いて、第 1 の実施形態に係る秘密再構成方法の概要を説明する。図 4 においては、メンバの人数は 3 人 (すなわち、演算記憶装置の数は 3 台) とし、各メンバは、もとの秘密情報 S を加算秘密分散法で分散させた分散情報 A, B, C をそれぞれ持っているものとする。もとの秘密情報 S を再構成する場合には、まず、各メンバが持っている分散情報 A, B, C を加算秘密分散法でさらに分散して、分散情報 A, B, C の分散情報を生成する。具体的に言えば、図 4

に符号①で示されるように、分散情報Aを分散して分散情報Aの分散情報 A_1 , A_2 , A_3 を生成し、分散情報Bを分散して分散情報Bの分散情報 B_1 , B_2 , B_3 を生成し、分散情報Cを分散して分散情報Cの分散情報 C_1 , C_2 , C_3 を生成する。次に、図4に符号②で示されるように、分散情報A, B, Cの分散情報を他のメンバに配布する。図4に符号③で示されるように、各メンバは、分散情報A, B, Cの分散情報 A_1 , B_1 , C_1 又は A_2 , B_2 , C_2 又は A_3 , B_3 , C_3 を受け取り、これらをもとに分散計算を行い、その分散計算の結果を出力する。次に、図4に符号④で示されるように、分散情報A, B, Cの分散情報 A_1 , B_1 , C_1 と、 A_2 , B_2 , C_2 と、 A_3 , B_3 , C_3 とをそれぞれ用いて分散計算した計算結果を集めることにより、もとの秘密情報Sを再構成する。

【0034】

図5は、本発明の第1の実施形態に係る秘密再構成方法を実施する構成（第1の実施形態に係る秘密再構成システム）を示すブロック図である。図5を用いて、第1の実施形態に係る秘密再構成方法を説明する。図5に示されるように、もとの秘密情報Sを再構成しようとする際に集まったn人のメンバ（すなわち、n台の演算記憶装置）には、それぞれ、分散計算で秘密情報を再構成する手段である分散秘密再構成計算部（すなわち、第1の実施形態に係る分散秘密再構成装置）301（301-1, 301-2, ..., 301-n）が備えられている。ここで、符号301-jは、メンバj（ $j=1, 2, \dots, n$ ）に備えられた分散秘密再構成計算部301を表わす。各メンバの分散秘密再構成計算部301-j（ $j=1, 2, \dots, n$ ）は、それぞれ他のメンバの分散秘密再構成計算部301と、図3で説明した秘密通信路303で接続されている。また、各メンバの分散秘密再構成計算部301-j（ $j=1, 2, \dots, n$ ）からの出力は、秘密再構成計算部302へ入力される。

【0035】

秘密再構成計算部302は、各メンバの分散秘密再構成計算部301-j（ $j=1, 2, \dots, n$ ）からの出力を受け取り、それら受け取ったn個の値を、n個の分散情報としたときの秘密情報の再構成を行う計算をし、その再構成された秘密情報を出力する。各メンバの分散秘密再構成計算部301-j（ $j=1, 2,$

..., n) から出力される値 (すなわち、秘密再構成計算の中間計算結果) を S_j ($j = 1, 2, \dots, n$) とすると、次式 (19) を用いて、もとの秘密情報 S を計算することができる。

【数 7】

$$\begin{aligned} S &= S_1 + S_2 + \dots + S_n \\ &= \sum_{j=1}^n S_j \quad (19) \end{aligned}$$

上記式 (19) における各演算は有限体 $GF(q)$ 上で行う。なお、以降の説明においては、断りがない限り、演算は、有限体 $GF(q)$ 上で行われるものとする。

【0036】

各メンバの分散秘密再構成計算部 301-j ($j = 1, 2, \dots, n$) における処理は、各メンバが、それぞれ他のメンバにはその処理の内容が分からないように行う。秘密再構成計算部 302 における処理は、処理を統合するセンター (メンバとは別の演算装置) のようなものを行ってもよいし、集まったメンバ (演算記憶装置) のうちの 1 人、又は、複数人で行ってもよい。ただし、秘密情報 S を必要としているメンバが行うのが望ましい。

【0037】

図 6 は、図 5 の分散秘密再構成計算部 301-j ($j = 1, 2, \dots, n$) の構成を示すブロック図である。図 6 を用いて分散秘密再構成計算部 301-j を説明する。図 6 に示されるように、分散秘密再構成計算部 301-j は、秘密分散計算部 401-j と、入力数が n 個である “(n) 加算部” 402-j とを有する。秘密分散計算部 401-j からの出力が “(n) 加算部” 402-j へ入力され、“(n) 加算部” 402-j からの出力が、分散秘密再構成計算部 301-j の出力となる。

【0038】

秘密分散計算部 401-j へは、メンバ j が持っているもとの秘密情報 S の分散情報 X_j が入力される。秘密分散計算部 401-j は、入力された分散情報 X_j を加算秘密分散法を用いて分散し、他のメンバと通信する秘密通信路 303 を

経由して配布する。分散情報 X_j の分散情報 $X_{j,n}$ の計算は、 $X_{j,1}, X_{j,2}, \dots, X_{j,n-1}$ を、乱数として有限体 $GF(q)$ 上の値を $n-1$ 個選び、次式 (20) で、 $X_{j,n}$ を求める。

$$X_{j,n} = X_j - (X_{j,1} + X_{j,2} + \dots + X_{j,n-1}) \quad \dots (20)$$

値 $X_{j,1}, X_{j,2}, \dots, X_{j,n}$ のうち、自分自身に対する分散情報 $X_{j,j}$ は、“(n) 加算部” 402-j へ出力し、その他の分散情報 $X_{j,p}$ ($p=1, 2, \dots, n$ であり、 $p \neq j$ であるもの) は、秘密通信路 303 を通して各メンバに配布される。

【0039】

“(n) 加算部” 402-j は、秘密分散計算部 401-j から、もとの秘密情報 S の分散情報 X_j の分散情報 $X_{j,j}$ を受け取る。さらに、秘密通信路 303 を経由して、他のメンバから配布された、もとの秘密情報 S の分散情報 X_p ($p=1, 2, \dots, n$ であり、 $p \neq j$ であるもの) の分散情報 $X_{1,j}, \dots, X_{j-1,j}, X_{j+1,j}, \dots, X_{n,j}$ を受け取る。これら n 個ある、もとの秘密情報 S の分散情報の分散情報 $X_{p,j}$ ($p=1, 2, \dots, n$) から、もとの秘密情報 S の分散情報 S_j (秘密情報 S の再構成時に得られる秘密情報 S の分散情報 S_j と、秘密情報 S の分散時に得られる秘密情報 S の分散情報 X_j とは異なるものである) を計算し出力する。“(n) 加算部” 402-j は、次式 (21) のような計算を行い、秘密情報 S の分散情報 S_j を出力する。

【数8】

$$\begin{aligned} S_j &= X_{1,j} + X_{2,j} + \dots + X_{n,j} \\ &= \sum_{p=1}^n X_{p,j} \quad (21) \end{aligned}$$

【0040】

[第1の実施形態の動作]

図7は、第1の実施形態に係る秘密再構成方法における動作を示すフローチャートである。ここで、もとの秘密情報 S を再構成するために集まったメンバ全員 (n 人のメンバ) が持つ分散情報を X_1, X_2, \dots, X_n とする。

【0041】

まず、各メンバが持つ分散情報 X_1, X_2, \dots, X_n を加算秘密分散方法を用いて分散し、他のメンバに配布する（ステップS501）。ステップS501は、図6の秘密分散計算部401-jにおける動作を示しており、各メンバの持つ分散情報 X_j から乱数生成及び上記式（20）を用いて分散情報 $X_{j,p}$ （ $p = 1, 2, \dots, n$ ）を計算し、他のメンバに対して配布する。

【0042】

次に、各メンバは、自分自身の分散情報 X_j の分散情報及び他のメンバから配布された分散情報、すなわち、分散情報 $X_{p,j}$ （ $p = 1, 2, \dots, n$ ）を用いて演算を施し、もとの秘密情報 S の分散情報 S_j を求める（ステップS502）。ステップS502は、図6の加算部402-jにおける動作を示しており、メンバ j は、他のメンバから配布された分散情報 $X_{p,j}$ （ $p = 1, 2, \dots, n$ ）（自分自身の分散情報 X_j の分散情報 $X_{j,j}$ が含まれている）から、上記式（21）を用いて計算する。その計算結果 S_j は、もとの秘密情報 S の分散情報となっている。

【0043】

次に、ステップS502で各メンバが計算した分散情報 S_j からもとの秘密情報 S を再構成する（ステップS503）。ステップS503は、図5の秘密再構成計算部302における動作を示しており、メンバ j がステップS502で計算した結果 S_j （ $j = 1, 2, \dots, n$ ）から、上記式（19）を用いて計算し、もとの秘密情報 S を得ることができる。

【0044】

[第1の実施形態の効果]

以上説明したように、第1の実施形態によれば、もとの秘密情報 S を再構成するために集まったメンバ（演算記憶装置）の持つ分散情報 X_j を、他のメンバに公開せずに、もとの秘密情報 S を再構成することができる。したがって、各メンバが持つ分散情報 X_j を、次の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを設けなくても、上記の効果を達成することができる。また、第1の実施形態においては、分散情報 X

j を持つメンバ全員が集まらなないと、もとの秘密情報 S を再構成することができないが、各メンバの匿名性は保たれており、さらに、秘密再構成の際のメンバ間の相互通信は、最初の分散情報を分散配布するための 1 回のみで済むため、通信量及び計算量の両方とも少ない。

【0045】

さらに、秘密情報 S の分散情報 X_j を持たない人（演算記憶装置）が、この再構成に参加しようとしても、秘密情報 S の再構成に失敗することから、第 1 の実施形態においては、集まった複数人数からなるグループ全員が正当メンバ（予め秘密情報 S の分散情報 X_j を配布されたメンバ）か、そうでない人（演算記憶装置）が混在するか、ということを認証するような機能が備わる。さらにまた、第 1 の実施形態においては、前述したように分散情報を再利用可能なので、この認証機能は、秘密情報 S の分散情報を更新せずとも何度も利用できる。また、この認証機能は、集まったメンバから他へ送信される情報は、認証（秘密情報 S の再構成）のたびに異なるので、盗聴による“なりすまし”に非常に強い。このような認証機能は、秘密分散法の秘密再構成の性質と、マルチパーティ・プロトコルによる分散計算の性質との単なる組み合わせによって得られる機能ではなく、新しい機能である。なお、上記認証機能は、「もとの秘密情報 S 」を照合秘密情報 S （予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いる利用形態であるので、もとの秘密情報 S を各メンバに秘密にしない場合であっても、実現できる。

【0046】

《第 2 の実施形態》

[第 2 の実施形態の概要]

本発明の第 2 の実施形態においては、もとの秘密情報 S を再構成する際に、もとの秘密情報 S を再構成するために集まったメンバ（演算記憶装置）が保有する分散情報を用いてマルチパーティ・プロトコルを実行することにより、各メンバが保有する分散情報を公開せずに、もとの秘密情報 S の再構成を行う。なお、第 2 の実施形態に係る秘密再構成方法は、秘密再構成システムにより実施される。第 2 の実施形態に係る秘密再構成システムは、各メンバ（演算記憶装置）である

分散秘密再構成装置（後述する分散秘密再構成計算部 6'0 1）と、メンバのいずれかに又はメンバとは別のセンターに備えられた演算装置（後述する秘密再構成計算部 6 0 2）とを主要な構成としている。

【0 0 4 7】

第 1 の実施形態は、複数のメンバからなるあるグループで、もとの秘密情報 S を、加算秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とした。これに対し、第 2 の実施形態は、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報 S を、 (k, n) しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。第 2 の実施形態の場合には、必ずしもメンバ全員（すなわち、 n 人のメンバ）が集まらなくとも、 k 人 ($k \leq n$) のメンバが集まれば、もとの秘密情報 S を再構成することができる。

【0 0 4 8】

第 2 の実施形態においては、もとの秘密情報 S を再構成させたいときに、集まったメンバ (t 人、 $t \geq k$) が分散情報を持ち寄り、上記式 (3) を用いてもとの秘密情報 S を再構成するが、この再構成時の計算を、マルチパーティ・プロトコルで分散計算することにより、集まった各メンバの分散情報を公開せずに、もとの秘密情報を再構成する。

【0 0 4 9】

[第 2 の実施形態の構成]

第 2 の実施形態は、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報 S を (k, n) しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。このグループには n 人のメンバがいるものとし、各メンバに秘密情報 S を分散させるときに用いたメンバ ID を m_1, m_2, \dots, m_n とする。メンバ ID が m_j ($j = 1, 2, \dots, n$) であるメンバに配布した、秘密情報 S の分散情報を X_{m_j} ($j = 1, 2, \dots, n$) とする。もとの秘密情報 S を再構成させたいときに、集まったメンバが t 人 ($t \geq k$) で、各メンバの持つ分散情報を持ち寄ったとする。このとき集まったメンバのメンバ ID を m'_1, m'_2, \dots, m'_t とし、集まったメンバが持つ分散

情報を $Xm'_1, Xm'_2, \dots, Xm'_t$ とする。また、集まったメンバのうち、どの2人のメンバ間にも、その2人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されているものとする。図3は、第2の実施形態において各メンバ間の通信に用いる秘密通信路303を示す図である。図3はにおいて、四角形で示されるブロックは集まったメンバを示し、 $m'_1, m'_2, \dots, m'_j, \dots, m'_t$ は、メンバIDを示し、両方向の矢印は、それぞれ対応するメンバ以外には通信内容を秘密とする秘密通信路303を示している。さらに、集まったt人のメンバに与えられたメンバID m'_1, m'_2, \dots, m'_t は公開された値であるものとする。

【0050】

図8は、本発明の第2の実施形態に係る秘密再構成方法を実施する構成（第2の実施形態に係る秘密再構成システム）を示すブロック図である。図8を用いて、第2の実施形態に係る秘密再構成方法を説明する。図8に示されるように、もとの秘密情報Sを再構成しようとする際に集まったメンバIDが m'_1, m'_2, \dots, m'_t であるt人のメンバ（すなわち、t台の演算記憶装置）は、それぞれ、分散計算により秘密情報を再構成する手段である分散秘密再構成計算部（すなわち、第2の実施形態に係る分散秘密再構成装置）601（601-1, 601-2, \dots , 601-t）が備えられている。分散秘密再構成計算部601-j（ $j=1, 2, \dots, t$ ）における処理は、メンバIDが m'_j であるメンバが行う。各メンバの分散秘密再構成計算部601-j（ $j=1, 2, \dots, t$ ）は、それぞれ他のメンバの分散秘密再構成計算部601とは、図3で示された秘密通信路303で接続されている。また、各メンバの分散秘密再構成計算部601-j（ $j=1, 2, \dots, t$ ）からの出力は、秘密再構成計算部602へ入力される。分散秘密再構成計算部601及び秘密再構成計算部602は、第1の実施形態における分散秘密再構成計算部301及び秘密再構成計算部302と、構成及び動作において異なる点を持つ。

【0051】

秘密再構成計算部602は、各メンバの分散秘密再構成計算部601-j（ $j=1, 2, \dots, t$ ）からの出力を受け取り、それら受け取ったt個の値を、t個

の分散情報としたときの秘密情報の再構成を行う計算をし、その再構成された秘密情報を入力する。各メンバの分散秘密再構成計算部 601-j ($j = 1, 2, \dots, t$) から出力される値を $S m'_j$ ($j = 1, 2, \dots, t$) とすると、上記式 (3) の $X m'_j$ を $S m'_j$ に置き換えた次式 (22) 及び (4) を用いて計算し、もとの秘密情報 S を出力する。

【数 9】

$$S = r m'_1 S m'_1 + r m'_2 S m'_2 + \dots + r m'_t S m'_t$$

$$= \sum_{j=1}^t r m'_j S m'_j \quad (22)$$

$$r m'_j = (m'_1 \times m'_2 \times \dots \times m'_t / m'_j) \\ \times ((m'_1 - m'_j) \times (m'_2 - m'_j) \times \dots \times (m'_{j-1} - m'_j) \times (m'_{j+1} - m'_j) \times \dots \times (m'_t - m'_j))$$

$$= \prod_{\substack{i=1 \\ i \neq j}}^t m'_i / (m'_i - m'_j) \quad (4)$$

上記式 (22) における各演算は有限体 $GF(q)$ 上で行う。以降の説明においては、断りがない限り、演算は、有限体 $GF(q)$ 上で行われるものとする。

【0052】

各メンバの分散秘密再構成計算部 601-j ($j = 1, 2, \dots, t$) における処理は、各メンバが、それぞれ他のメンバにはその処理の内容が分からないように行う。秘密再構成計算部 602 における処理は、処理を統合するセンター（メンバとは別の演算装置）のようなものを行ってもよいし、集まったメンバ（演算記憶装置）のうち、だれか 1 人、又は、複数人で行ってもよい。ただし、秘密情報 S を必要としているメンバが行うのが望ましい。

【0053】

図 9 は、図 8 の分散秘密再構成計算部 601-j ($j = 1, 2, \dots, t$) の構成を示すブロック図である。図 9 を用いて分散秘密再構成計算部 601-j を説明する。図 9 に示されるように、分散秘密再構成計算部 601-j は、秘密分散計算部 701-j と、線形結合計算部 702-j とを有する。秘密分散計算部 701-j からの出力が線形結合計算部 702-j へ入力され、線形結合計算部 7

02-jからの出力が、分散秘密再構成計算部701-jの出力となる。

【0054】

秘密分散計算部701-jへは、メンバIDが m'_j であるメンバが持つものの秘密情報Sの分散情報 Xm'_j が入力される。秘密分散計算部701-jは、入力された分散情報 Xm'_j を (k', t) しきい値秘密分散法 $(k' \leq t)$ を用いて分散し、他のメンバと通信する秘密通信路303を経由して配布する。分散するときの計算においては、上記式(6)の m_j が m'_j に置き換わり、 k が k' に置き換わった $k'-1$ 次多項式である次式(23)を作る。

【数10】

$$f_{m'_j}(x) = Xm'_j + R_{m'_j,1}x + R_{m'_j,2}x^2 + \dots + R_{m'_j,k'-1}x^{k'-1} \quad (23)$$

ここで、 $R_{m'_j,1}, R_{m'_j,2}, \dots, R_{m'_j,k'-1}$ は、乱数として選ばれた有限体GF(q)上の $k'-1$ 個の値である。

【0055】

そして、メンバIDが m'_p ($p = 1, 2, \dots, t$)であるメンバに対して配布する分散情報 $Xm'_{j,p}$ を、上記式(23)を用いて次式(24)のように計算する(上記式(7)参照)。

【数11】

$$\begin{aligned} Xm'_{j,p} &= f_{m'_j}(m'_p) \\ &= Xm'_j + R_{m'_j,1}(m'_p) + R_{m'_j,2}(m'_p)^2 + \dots + R_{m'_j,k'-1}(m'_p)^{k'-1} \end{aligned} \quad (24)$$

【0056】

自分自身に対する分散情報 $Xm'_{j,j}$ は、線形結合計算部702-jへ出力し、その他の分散情報 $Xm'_{j,p}$ ($p = 1, 2, \dots, t$ であり、 $p \neq j$ であるもの)を秘密通信路303を通して各メンバに配布する。

【0057】

線形結合計算部702-jは、秘密分散計算部701-jから、もとの秘密情報Sの分散情報 Xm'_j の分散情報 $Xm'_{j,j}$ を受け取る。さらに、秘密通信路303を経由して、他のメンバから配布された、もとの秘密情報Sの分散情報X

m'_j の分散情報 $Xm'_{1,j}, \dots, Xm'_{j-1,j}, Xm'_{j+1,j}, \dots, Xm'_{t,j}$ を受け取る。これら t 個ある、もとの秘密情報 S の分散情報 Xm'_j の分散情報 Xm'_p, j ($p = 1, 2, \dots, t$)、から、もとの秘密情報 S の分散情報 Sm'_j (秘密情報 S の再構成時に得られる秘密情報 S の分散情報 Sm'_j と、秘密情報 S の分散時に得られる秘密情報 S の分散情報 Xm'_j とは異なるものである) を計算し出力する。線形結合計算部 702-j は、次式 (25) 及び (26) のような計算を行う。

【数 12】

$$\begin{aligned} Sm'_j &= r m'_1 Xm'_{1,j} + r m'_2 Xm'_{2,j} + \dots + r m'_t Xm'_{t,j} \\ &= \sum_{p=1}^t r m'_p Xm'_{p,j} \quad (25) \end{aligned}$$

$$\begin{aligned} r m'_p &= (m'_1 \times m'_2 \times \dots \times m'_t / m'_p) \\ &\quad / ((m'_1 - m'_p) \times (m'_2 - m'_p) \times \dots \times (m'_{p-1} - m'_p) \times (m'_{p+1} - m'_p) \times \dots \times (m'_t - m'_p)) \\ &= \prod_{\substack{i=1 \\ i \neq p}}^t m'_i / (m'_i - m'_p) \quad (26) \end{aligned}$$

ここで、各メンバ ID m'_1, m'_2, \dots, m'_t は公開された値であるので、上記式 (26) の $r m'_p$ を計算することができる。

【0058】

[第 2 の実施形態の動作]

図 10 は、第 2 の実施形態に係る秘密再構成方法における動作を示すフローチャートである。ここで、もとの秘密情報 S を再構成するために集まった t 人のメンバのメンバ ID を m'_1, m'_2, \dots, m'_t とし、各メンバが持つ分散情報を $Xm'_1, Xm'_2, \dots, Xm'_t$ とする。

【0059】

第 2 の実施形態に係る秘密再構成方法においては、図 10 に示されるように、まず、各メンバが持つ分散情報を (k', t) しきい値秘密分散法を用いて分散し、他のメンバに配布する (ステップ S801)。ステップ S801 は、図 9 の秘密分散計算部 701-j における動作を示しており、メンバ ID が m'_j (j

$= 1, 2, \dots, t$) であるメンバの持つ分散情報 $X_{m'j}$ を上記式 (23) を用いて分散し、メンバ ID が m'_p ($p = 1, 2, \dots, t$) であるメンバに対し、上記式 (24) で計算される $X_{m'j,p}$ を配布する。

【0060】

次に、各メンバは、公開されている集まったメンバのメンバ ID、自分自身の分散情報 $X_{m'j}$ の分散情報及び他のメンバから配布された分散情報、すなわち、分散情報 $X_{m'p,j}$ ($p = 1, 2, \dots, t$) を用いて演算を施し、もとの秘密情報 S の分散情報 $S_{m'j}$ である値を求める (ステップ S802)。ステップ S802 は、図 9 の線形結合計算部 702-j における動作を示しており、メンバ ID が m'_j ($j = 1, 2, \dots, t$) であるメンバは、他のメンバから配布された分散情報 $X_{m'p,j}$ ($p = 1, 2, \dots, t$) (自分自身の分散情報 $X_{m'j}$ の分散情報 $X_{m'j,j}$ が含まれている)、及び公開されているメンバ ID m'_p ($p = 1, 2, \dots, t$) から、上記式 (25) を用いて計算する。その計算結果 $S_{m'j}$ は、もとの秘密情報 S の分散情報となっている。

【0061】

次に、ステップ S802 で、各メンバが計算した分散情報からもとの秘密情報 S を再構成する (ステップ S803)。ステップ S803 は、図 8 の秘密再構成計算部 602 における動作を示しており、メンバ ID が m'_j ($j = 1, 2, \dots, t$) であるメンバがステップ S802 で計算した結果 $S_{m'j}$ ($j = 1, 2, \dots, t$) から、上記式 (22) を用いて計算し、もとの秘密情報 S を得ることができる。

【0062】

[第 2 の実施形態の効果]

以上説明したように、第 2 の実施形態によれば、第 1 の実施形態と同様に、もとの秘密情報 S を再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報 S を再構成することができる。したがって、各メンバが持つ分散情報を、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを設けなくても、上記の効果を達成することができる。

【0063】

また、上記第1の実施形態においては、もとの秘密情報Sは、各メンバに加算秘密分散法を用いて分散させていたので、メンバ全員が集まらなないと、もとの秘密情報Sを再構成することができなかったが、第2の実施形態の場合、必ずしもメンバ全員、すなわちn人のメンバが集まらなくとも、k人 ($k \leq n$) 以上のメンバが集まれば、もとの秘密情報Sを再構成することができる。

【0064】

このように、第2の実施形態においては、集まったメンバのメンバIDを公開するので、集まったメンバを匿名にすることはできないが（少なくとも、もとの秘密情報Sを秘密分散させるときのメンバIDは分かってしまうが）、秘密再構成の際のメンバ間の相互通信は、最初の分散情報を分散配布するための1回のみで済むため、通信量及び計算量の両方とも少なく、しかも、必ずしもメンバ全員、すなわちn人が集まらなくとも、k人 ($k \leq n$) が集まれば、もとの秘密情報Sを再構成することができる。

【0065】

さらに、第2の実施形態においては、第1の実施形態と同様に、予め秘密情報Sの分散情報を持たない人（演算記憶装置）が、この再構成に参加しようとしても、秘密情報Sの再構成に失敗することから、集まった複数人数からなるグループ全員が正当メンバ（予め秘密情報Sの分散情報を配布されたメンバ）か、そうでない人（演算記憶装置）が混在するか、ということを認証するような機能が備わる。さらにまた、第2の実施形態においては、前述のように分散情報を再利用可能なので、この認証機能は、秘密情報Sの分散情報を更新せずとも何度も利用できる。また、この認証機能は、集まったメンバから他へ送信される情報は、認証（秘密情報Sの再構成）のたびに異なるので、盗聴による“なりすまし”に非常に強い。このような認証機能は、秘密分散法の秘密再構成の性質と、マルチパーティ・プロトコルによる分散計算の性質との単なる組み合わせによって得られる機能ではなく、新しい機能である。なお、上記認証機能は、「もとの秘密情報S」を照合秘密情報S（予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いる利用形態であるので、もとの秘

密情報 S を各メンバに秘密にしない場合であっても、実現できる。

【0066】

《第3の実施形態》

[第3の実施形態の概要]

本発明の第3の実施形態においては、上記第1及び第2の実施形態と同様に、もとの秘密情報 S を再構成する際に、もとの秘密情報 S を再構成するために集まったメンバ（演算記憶装置）が保有する分散情報を用いてマルチパーティ・プロトコル（前述のマルチパーティ・プロトコルの第1方式）を実行することにより、各メンバが保有する分散情報を公開せずにもとの秘密情報 S の再構成を行う。なお、第3の実施形態に係る秘密再構成方法は、秘密再構成システムにより実施される。第3の実施形態に係る秘密再構成システムは、仮メンバ ID 生成部（後述する図12における符号901）と、各メンバ（演算記憶装置）である分散秘密再構成装置（後述する分散秘密再構成計算部902）と、メンバのいずれかに又はメンバとは別のセンターに備えられた演算装置（後述する秘密再構成計算部903）とを主要な構成としている。

【0067】

第1の実施形態は、複数のメンバからなるあるグループで、もとの秘密情報 S を、加算秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提としていた。これに対し、第3の実施形態は、第2の実施形態と同様に、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報 S を、 (k, n) しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。第3の実施形態の場合には、必ずしもメンバ全員（すなわち、 n 人のメンバ）が集まらなくとも、 k 人 ($k \leq n$) のメンバが集まれば、もとの秘密情報 S を再構成することができる。

【0068】

また、上記第2の実施形態においては、集まったメンバのメンバ ID を公開して秘密再構成を行っていたが、第3の実施形態においては、各メンバが保有する分散情報だけでなく、メンバ ID をも公開せずに秘密情報の再構成を行なう。第3の実施形態においては、マルチパーティ・プロトコルは、前述したマルチパー

ティ・プロトコルの第1方式を使用する。

【0069】

[第3の実施形態の構成]

第3の実施形態は、上記第2の実施形態と同様に、複数のメンバ（演算記憶装置）からなるあるグループで、もとの秘密情報 S を (k, n) しきい値秘密分散法を用いて分散し、各メンバに分散情報が秘密裏に配布されている状態を前提とする。このグループには n 人のメンバがいるものとし、各メンバに秘密情報 S を分散させるときに用いたメンバIDを m_1, m_2, \dots, m_n とする。メンバIDが m_j ($j = 1, 2, \dots, n$)であるメンバに配布した、秘密情報 S の分散情報を Xm_j ($j = 1, 2, \dots, n$)とする。もとの秘密情報 S を再構成させたいときに、集まったメンバが t 人 ($t \geq k$)で、各メンバの持つ分散情報を持ち寄ったとする。このとき集まったメンバのメンバIDを m'_1, m'_2, \dots, m'_t とし、そのメンバが持つ分散情報を $Xm'_1, Xm'_2, \dots, Xm'_t$ とする。また、上記第1及び第2の実施形態と同様に、集まったメンバのうち、どの2人のメンバ間にも、その2人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されているものとする（図3参照）。ただし、第2の実施形態とは異なり、集まったメンバのメンバID— m'_1, m'_2, \dots, m'_t は公開されず、どのメンバIDを持つメンバが集まっているかを知ることができないようになっている。また、以降の計算（加算「+」及び乗算「 \times 」などの四則演算）においては、有限体 $GF(q)$ 上の演算を行うものとする。

【0070】

次に、図11を用いて、第3の実施形態に係る秘密再構成方法の概要を説明する。図11においては、メンバの人数は3人（すなわち、演算記憶装置の数は3台）とし、各メンバは、もとの秘密情報 S をしきい値秘密分散法で分散させた分散情報 Xm_1, Xm_2, Xm_3 及びメンバID— m_1, m_2, m_3 をそれぞれ持っているものとする。もとの秘密情報 S を再構成する場合には、各メンバが持っている分散情報を、さらにしきい値秘密分散法で分散する。具体的に言えば、図11に符号①で示されるように、秘密情報 S の分散情報 Xm_1 から秘密分散法により分散情報 Xm_1 の分散情報 $Xm_{1,1}, Xm_{1,2}, Xm_{1,3}$ を生成し、

秘密情報 S の分散情報 X_{m2} から秘密分散法により分散情報 X_{m2} の分散情報 $X_{m2,1}$, $X_{m2,2}$, $X_{m2,3}$ を生成し、秘密情報 S の分散情報 X_{m3} から秘密分散法により分散情報 X_{m3} の分散情報 $X_{m3,1}$, $X_{m3,2}$, $X_{m3,3}$ を生成する。さらに、メンバ ID_{m1} から秘密分散法によりメンバ ID_{m1} の分散情報 $m_{1,1}$, $m_{1,2}$, $m_{1,3}$ を生成し、メンバ ID_{m2} から秘密分散法によりメンバ ID_{m2} の分散情報 $m_{2,1}$, $m_{2,2}$, $m_{2,3}$ を生成し、メンバ ID_{m3} から秘密分散法によりメンバ ID_{m3} の分散情報 $m_{3,1}$, $m_{3,2}$, $m_{3,3}$ を生成する。そして、図 11 に符号②で示されるように、秘密情報 S の分散情報 X_{m1} , X_{m2} , X_{m3} の分散情報 $X_{m1,1}$, $X_{m1,2}$, $X_{m1,3}$ 及び $X_{m2,1}$, $X_{m2,2}$, $X_{m2,3}$ 及び $X_{m3,1}$, $X_{m3,2}$, $X_{m3,3}$ を他のメンバに配布する。次に、図 11 に符号③で示されるように、各メンバは、受け取った分散情報の分散情報 $X_{m1,1}$, $X_{m2,1}$, $X_{m3,1}$ 及び $X_{m1,2}$, $X_{m2,2}$, $X_{m3,2}$ 及び $X_{m1,3}$, $X_{m2,3}$, $X_{m3,3}$ 、並びに、メンバ ID の分散情報 $m_{1,1}$, $m_{2,1}$, $m_{3,1}$ 及び $m_{1,2}$, $m_{2,2}$, $m_{3,2}$ 及び $m_{1,3}$, $m_{2,3}$, $m_{3,3}$ をもとに、分散計算を行い、その分散計算の結果を出力する。次に、図 11 に符号④で示されるように、各メンバは、分散情報 $X_{m1,1}$, $X_{m2,1}$, $X_{m3,1}$ 及び $X_{m1,2}$, $X_{m2,2}$, $X_{m3,2}$ 及び $X_{m1,3}$, $X_{m2,3}$, $X_{m3,3}$ 、並びに、分散情報 $m_{1,1}$, $m_{2,1}$, $m_{3,1}$ 及び $m_{1,2}$, $m_{2,2}$, $m_{3,2}$ 及び $m_{1,3}$, $m_{2,3}$, $m_{3,3}$ を用いた分散計算の計算結果を集めることにより、もとの秘密情報 S を再構成する。

【0071】

図 12 は、本発明の第 3 の実施形態に係る秘密再構成方法を実施する構成（第 3 の実施形態に係る秘密再構成システム）を示すブロック図である。図 12 を用いて、第 3 の実施形態に係る秘密再構成方法を説明する。図 12 に示されるように、もとの秘密情報 S を再構成しようとする際に集まったメンバ ID が m'_1 , m'_2 , ..., m'_t であるメンバ（すなわち、 t 台の演算記憶装置）は、それぞれ、分散計算により秘密情報を再構成する手段である分散秘密再構成計算部（すなわち、第 3 の実施形態に係る分散秘密再構成装置）902（902-1, 902

ー2, ..., 902-t) が備えられている。また、秘密再構成方法を実施するシステムは、仮メンバID生成部901及び秘密再構成計算部903を有している。分散秘密再構成計算部902、及び秘密再構成計算部903は、第1及び第2の実施形態における分散秘密再構成計算部301及び601、並びに、秘密再構成計算部302及び602と、構成や動作に異なる点を持つ。仮メンバID生成部901は、集まった各メンバの分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) とそれぞれ接続されている。各メンバの分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) は、それぞれ他のメンバの分散秘密再構成計算部902とは、図3で説明した秘密通信路303で接続されている。また、各メンバの分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) からの出力は、秘密再構成計算部903へ入力される。

【0072】

仮メンバID生成部901は、これら集まったメンバt人に対し、互いに重複した値をとらないようなt個の値 d_1, d_2, \dots, d_t を生成し、これらの値を仮メンバIDとして、分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) へそれぞれ出力する。もし、IPアドレスなどの互いに重複した値をとらないようなt個の値が既に利用できる状態であるならば、値を生成する代わりに、各分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) からそのような値を申請させて、それを仮メンバID $_d_1, d_2, \dots, d_t$ として利用することもできる。さらに、これら仮メンバID $_d_1, d_2, \dots, d_t$ は公開され、それぞれがどの仮メンバIDを持つかは、集まった各メンバにとっては既知の値であるとする。その公開方法は、例えば、図12に破線で示される制御信号を用いて、分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) が、仮メンバID $_d_j$ ($j=1, 2, \dots, t$) に対応しているかを通知する方法を採ることにより公開することもできる。仮メンバID生成部901は、仮メンバID $_d_1, d_2, \dots, d_t$ を各分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) に対応付け、仮メンバIDを公開する機能を持つ。

【0073】

各メンバの分散秘密再構成計算部902-j ($j=1, 2, \dots, t$) は、仮メ

ンバIDが d_j であるメンバの処理部分であり、仮メンバID生成部901から、自分に対する仮メンバIDを受け取り、各自処理（詳細は後述）した出力結果と仮メンバID $_d_j$ を、秘密再構成計算部903へ出力する。

【0074】

秘密再構成計算部903は、各メンバの分散秘密再構成計算部902-j ($j = 1, 2, \dots, t$) からの出力を受け取り、それら受け取った t 個の情報を、 t 個の分散情報としたときの秘密情報の再構成を行う計算をし、その再構成された秘密情報を出力する。各メンバの分散秘密再構成計算部902-j ($j = 1, 2, \dots, t$) から出力される値を $S d_j$ ($j = 1, 2, \dots, t$) 及び仮メンバID $_d_j$ とすると、上記式(22)及び(4)において、 m'_j を d_j に、 $S m'_j$ を $S d_j$ に置き換えた次式(27)及び(28)を計算し、もとの秘密情報 S を出力する。

【数13】

$$\begin{aligned} S &= r d_1 S d_1 + r d_2 S d_2 + \dots + r d_t S d_t \\ &= \sum_{j=1}^t r d_j S d_j \quad (27) \end{aligned}$$

$$\begin{aligned} r d_j &= (d_1 \times d_2 \times \dots \times d_t / d_j) \\ &\quad / ((d_1 - d_j) \times (d_2 - d_j) \times \dots \times (d_{j-1} - d_j) \times (d_{j+1} - d_j) \times \dots \times (d_t - d_j)) \\ &= \prod_{\substack{i=1 \\ i \neq j}}^t d_i / (d_i - d_j) \quad (28) \end{aligned}$$

上記式(27)及び(28)における各演算は有限体GF(q)上で行う。

【0075】

各メンバの分散秘密再構成計算部902-j ($j = 1, 2, \dots, t$) における処理は、各メンバが、それぞれ他のメンバにはその処理の内容が分からないように行う。仮メンバID生成部901及び秘密再構成計算部903における処理は、処理を統合するセンター（メンバとは別の演算装置）のようなものを行ってもよいし、集まったメンバ（演算記憶装置）のうち、だれか1人、又は、複数人で行ってもよい。ただし、秘密再構成計算部903における処理は、秘密情報 S を必要としているメンバが行うのが望ましい。

【0076】

図13は、図12の分散秘密再構成計算部902-j ($j = 1, 2, \dots, t$)の構成を示すブロック図である。図13を用いて分散秘密再構成計算部902-j ($j = 1, 2, \dots, t$)を説明する。図13に示されるように、分散秘密再構成計算部902-jは、秘密分散計算部1001-jと、分散処理部1002-jとを有する。分散秘密再構成計算部902-jへの入力は、秘密分散計算部1001-jへ入力され、秘密分散計算部1001-jからの出力が分散処理部1002-jへ入力される。分散処理部1002-jからの出力が、分散秘密再構成計算部902-jの出力となる。秘密分散計算部1001-jには、図12の仮メンバID生成部901から出力される仮メンバID $_d_j$ が入力される。さらに、秘密分散計算部1001-jには、仮メンバIDが d_j で与えられるメンバの持つメンバID $_m'_j$ と、もとの秘密情報Sの分散情報 Xm'_j とが入力される。秘密分散計算部1001-jは、入力された分散情報 Xm'_j 及びメンバID $_m'_j$ を、それぞれ(k', t)しきい値秘密分散法を用いて分散し、他のメンバと通信する秘密通信路303を経由して配布する。第3の実施形態の場合には、第2の実施形態の場合とは異なり、分散乗算を行わなければならないので、この秘密分散法のしきい値 k' は、

$$k' \leq (t+1)/2 \quad \dots (29)$$

を満たさなければならない。(上記式(11)参照)。上記式(29)の演算は、有限体GF(q)上の演算ではなく、通常の実数、整数演算である。

【0077】

入力された分散情報 Xm'_j を分散するときの計算方法は、第2の実施形態と同様に、上記式(23)のような $k'-1$ 次多項式である次式(29')を作ることにより行う。

【数14】

$$f_{jd_j}(x) = Xm'_j + R_1 d_{j,1} x + R_1 d_{j,2} x^2 + \dots + R_1 d_{j,k'-1} x^{k'-1} \quad (29')$$

ただし、メンバID $_m'_p$ ($p = 1, 2, \dots, t$)は非公開の値であるので、代わりに仮メンバID $_d_p$ ($p = 1, 2, \dots, t$)を用いる。ここで、 $R_1 d$

$j, 1, R_1 d_{j, 2}, \dots, R_1 d_{j, k'-1}$ は、乱数として選ばれた有限体 $GF(q)$ 上の $k'-1$ 個の値である。

【0078】

そして、仮メンバ ID が d_p ($p = 1, 2, \dots, t$) であるメンバに対して配布する分散情報 $Xm'_{j, p}$ を、上記式 (29') を用いて次式 (30) のように計算する。

【数15】

$$\begin{aligned} Xm'_{j, p} &= f_1 d_j(d_p) \\ &= Xm'_j + R_1 d_{j, 1}(d_p) + R_1 d_{j, 2}(d_p)^2 + \dots + R_1 d_{j, k'-1}(d_p)^{k'-1} \end{aligned} \quad (30)$$

【0079】

入力されるメンバ $ID_m'_j$ を分散するときは、同様に、次式 (31) なる $k'-1$ 次多項式を作る。

【数16】

$$f_2 d_j(x) = m'_j + R_2 d_{j, 1} x + R_2 d_{j, 2} x^2 + \dots + R_2 d_{j, k'-1} x^{k'-1} \quad (31)$$

ここで、 $R_2 d_{j, 1}, R_2 d_{j, 2}, \dots, R_2 d_{j, k'-1}$ は、乱数として選ばれた有限体 $GF(q)$ 上の $k'-1$ 個の値である。

【0080】

そして、仮メンバ ID が d_p ($p = 1, 2, \dots, t$) であるメンバに対して配布する分散情報 $m'_{j, p}$ を、上記式 (31) を用いて次式 (32) のように計算する。

【数17】

$$\begin{aligned} m'_{j, p} &= f_2 d_j(d_p) \\ &= m'_j + R_2 d_{j, 1}(d_p) + R_2 d_{j, 2}(d_p)^2 + \dots + R_2 d_{j, k'-1}(d_p)^{k'-1} \end{aligned} \quad (32)$$

【0081】

自分自身に対する分散情報 $Xm'_{j, j}$ 及び $m'_{j, j}$ は、分散処理部 1002-j へ出力し、その他の分散情報 $Xm'_{j, p}$ 及び $m'_{j, p}$ ($p = 1, 2, \dots, t$ で

あり、 $p \neq j$ であるもの)を秘密通信路303を通して各メンバに配布する(他のメンバの分散処理部1002-p ($p = 1, 2, \dots, t$ であり、 $p \neq j$ であるもの)へ送信する)。

【0082】

分散処理部1002-jは、秘密分散計算部1001-jから、メンバIDの分散情報 $m'_{j,j}$ 、及び、もとの秘密情報Sの分散情報の分散情報 $Xm'_{j,j}$ を受け取る。さらに、秘密通信路303を経由して、他のメンバから配布された(他のメンバの秘密分散計算部1001-p ($p = 1, 2, \dots, t$ であり、 $p \neq j$ であるもの)から送信された)、他のメンバのメンバIDの分散情報 $m'_{1,j}$ 、 $m'_{2,j}$ 、 \dots 、 $m'_{t,j}$ 、及び、もとの秘密情報Sの分散情報の分散情報である $Xm'_{1,j}$ 、 $Xm'_{2,j}$ 、 \dots 、 $Xm'_{t,j}$ を受け取る。これらメンバIDの分散情報 $m'_{p,j}$ ($p = 1, 2, \dots, t$)と、もとの秘密情報Sの分散情報の分散情報 $Xm'_{p,j}$ ($p = 1, 2, \dots, t$)、から、もとの秘密情報Sの分散情報となる Sd_j を計算して出力する。すなわち、集まったメンバのメンバID $m'_{1,j}$ 、 $m'_{2,j}$ 、 \dots 、 $m'_{t,j}$ 及び分散情報 $Xm'_{1,j}$ 、 $Xm'_{2,j}$ 、 \dots 、 $Xm'_{t,j}$ を分散させたまま、上記式(3)で示される式の分散計算を行う。その結果得られる値Sは、分散秘密情報 Sd_1 、 Sd_2 、 \dots 、 Sd_t として、各メンバがそれぞれ持っていることになる。

【0083】

図14は、図13の分散処理部1002-j ($j = 1, 2, \dots, t$)の構成を示すブロック図である。図14を用いて分散処理部1002-j ($j = 1, 2, \dots, t$)の構成を説明する。分散処理部1002-jは、t個の項計算部1101-j-a ($a = 1, 2, \dots, t$)と、t個の情報が入力される“(t)加算部”1102-jとを有する。秘密分散計算部1001-jからの出力 $Xm'_{j,j}$ 及び $m'_{j,j}$ 、さらに、秘密通信路303を経由して、他のメンバから配布された(他のメンバの秘密分散計算部1001-p ($p = 1, 2, \dots, t$ であり、 $p \neq j$ であるもの)から送信された)、他のメンバのメンバIDの分散情報 $m'_{1,j}$ 、 $m'_{2,j}$ 、 \dots 、 $m'_{t,j}$ 、及び、もとの秘密情報Sの分散情報の分散情報 $Xm'_{1,j}$ 、 $Xm'_{2,j}$ 、 \dots 、 $Xm'_{t,j}$ は、項計算部1101-j-a

($a = 1, 2, \dots, t$) へ入力される。項計算部 $1101-j-a$ ($a = 1, 2, \dots, t$) からの出力は、“(t) 加算部” $1102-j$ へ入力され、“(t) 加算部” $1102-j$ からの出力が、分散処理部 $1002-j$ の出力となる。項計算部 $1101-j-a$ は、それぞれ、他のメンバの秘密分散計算部 $1001-p$ 及び項計算部 $1101-p-a$ ($p = 1, 2, \dots, t$ であり、 $p \neq j$ であるもの) との秘密通信路 303 を持っている。

【0084】

“(t) 加算部” $1102-j$ は、項計算部 $1101-1-a$ ($a = 1, 2, \dots, t$) からそれぞれ一つずつの出力 (合計 t 個) を受け取り、それらをすべて (t 個) 加算する。すなわち、項計算部 $1101-j-a$ からの出力を Y_a ($a = 1, 2, \dots, t$) とすると、“(t) 加算部” $1102-j$ は、次式 (33)、すなわち、

$$Sd_j = Y_1 + Y_2 + \dots + Y_t \quad \dots (33)$$

を計算し、計算結果である Sd_j を出力する。

【0085】

図 15 は、図 14 の項計算部 $1101-j-a$ ($a = 1, 2, \dots, t$) の構成を示すブロック図である。次に、図 15 を用いて項計算部 $1101-j-a$ ($a = 1, 2, \dots, t$) の構成を説明する。項計算部 $1101-j-a$ ($a = 1, 2, \dots, t$) は、差分計算部 $1201-j-a$ と、 $t-1$ 個の情報が入力される“(t-1) 分散乗算部” $1202-j-a$ と、 $t-1$ 個の情報が入力される“(t-1) 分散乗算部” $1204-j-a$ と、分散逆元計算部 $1203-j-a$ と、2 個の情報が入力される“(2) 分散乗算部” $1205-j-a$ と、2 個の情報が入力される“(2) 分散乗算部” $1206-j-a$ とを有する。項計算部 $1101-j-a$ ($a = 1, 2, \dots, t$) へ入力される $m'_{1,j}, m'_{2,j}, \dots, m'_{t,j}$ は、秘密通信路 303 を通して、差分計算部 $1201-j-a$ へ入力され (ただし、 $m'_{j,j}$ は、秘密分散計算部 $1001-j$ からの入力)、差分計算部 $1201-j-a$ からの出力は、“(t-1) 分散乗算部” $1202-j-a$ へ入力される。“(t-1) 分散乗算部” $1202-j-a$ からの出力は、分散逆元計算部 $1203-j-a$ へ入力され、分散逆元計算部 $1203-j-a$

からの出力は、“(2) 分散乗算部” 1205-j-a へ入力される。また、項計算部 1101-j-a ($a=1, 2, \dots, t$) へ秘密通信路 303 を通して入力される $m'_{1,j}, m'_{2,j}, \dots, m'_{t,j}$ (ただし、 $m'_{j,j}$ は、秘密分散計算部 1001-j からの入力) のうち $m'_{a,j}$ 以外の値は、“(t-1) 分散乗算部” 1204-j-a へも入力され、“(t-1) 分散乗算部” 1204-j-a からの出力は、分散逆元計算部 1203-j-a からの出力とともに、“(2) 分散乗算部” 1205-j-a へ入力される。“(2) 分散乗算部” 1205-j-a からの出力は、項計算部 1101-j-a ($a=1, 2, \dots, t$) へ秘密通信路 303 を通して入力される $Xm'_{a,j}$ (ただし、項計算部 1101-j-j への入力 $Xm'_{j,j}$ は、秘密分散計算部 1001-j からの入力) とともに、“(2) 分散乗算部” 1206-j-a へ入力される。“(2) 分散乗算部” 1206-j-a からの出力が、項計算部 1101-j-a の出力となる。また、“(t-1) 分散乗算部” 1202-j-a, 1204-j-a、分散逆元計算部 1203-j-a、“(2) 分散乗算部” 1205-j-a, 1206-j-a はそれぞれ、他のメンバの、“(t-1) 分散乗算部” 1202-p-a, 1204-p-a、分散逆元計算部 1203-p-a、“(2) 分散乗算部” 1205-p-a, 1206-p-a ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) との秘密通信路 303 を持っている。

【0086】

差分計算部 1201-j-a は、項計算部 1101-j-a へ入力されるメンバ ID $m'_{1,j}, m'_{2,j}, \dots, m'_{t,j}$ を受け取り、それぞれのメンバ ID $m'_{1,j}, m'_{2,j}, \dots, m'_{t,j}$ と $m'_{a,j}$ の差分を計算する。ただし、 $m'_{a,j}$ 同士の差分は計算しない。すなわち、 $(m'_{1,j} - m'_{a,j}), (m'_{2,j} - m'_{a,j}), \dots, (m'_{(a-1),j} - m'_{a,j}), (m'_{(a+1),j} - m'_{a,j}), \dots, (m'_{t,j} - m'_{a,j})$ の $t-1$ 個の差分の計算を行う。これら $t-1$ 個の計算結果は、“(t-1) 分散乗算部” 1202-j-a へ出力される。

【0087】

“(t-1) 分散乗算部” 1202-j-a, 1204-j-a は、内部的に

は同じ構成であり、 $t-1$ 個の入力を受け取り、それらの入力と秘密通信路 303 からの情報を用いて、 $t-1$ 個の要素の分散乗算を行い、その計算結果を出力する。“ $(t-1)$ 分散乗算部” 1202-j-a, 1204-j-a へ入力される値を $A_{1,j}, A_{2,j}, \dots, A_{(t-1),j}$ とする。 $A_{i,j}$ ($i=1, 2, \dots, t-1$) と、他のメンバの “ $(t-1)$ 分散乗算部” 1202-p-a, 1204-p-a へ入力される $A_{i,p}$ ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) の、 t 個の値 $A_{i,p}$ ($p=1, 2, \dots, t$) を分散情報として再構成されるようなもとの秘密を A_j とすると、“ $(t-1)$ 分散乗算部” 1202-j-a, 1204-j-a は、 A_j ($i=1, 2, \dots, t-1$) をすべて乗算した値

$$B = A_1 \times A_2 \times \dots \times A_{t-1}$$

の、仮メンバ ID が d_j であるメンバに対する分散情報 B_j を計算することとなる。“ $(t-1)$ 分散乗算部” 1202-j-a は、差分計算部 1201-j-a からの $t-1$ 個の出力を受け取り、それらを用いて計算し、その計算結果を分散逆元計算部 1203-j-a へ出力する。“ $(t-1)$ 分散乗算部” 1202-j-a は、他のメンバの “ $(t-1)$ 分散乗算部” 1202-p-a ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) と秘密通信路 303 を経由して必要な情報をやり取りする。“ $(t-1)$ 分散乗算部” 1204-j-a は、項計算部 1101-j-a へ入力される $m'_{1,j}, m'_{2,j}, \dots, m'_{t,j}$ のうち、 $m'_{a,j}$ 以外のものを受け取り、それらを用いて計算し、その計算結果を “ (2) 分散乗算部” 1205-j-a へ出力する。“ $(t-1)$ 分散乗算部” 1204-j-a は、他のメンバの “ $(t-1)$ 分散乗算部” 1204-p-a ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) と秘密通信路 303 を経由して必要な情報をやり取りする。

【0088】

分散逆元計算部 1203-j-a は、“ $(t-1)$ 分散乗算部” 1202-j-a からの出力を受け取り、その値と秘密通信路 303 からの情報を用いて分散計算し、その計算結果を、“ (2) 分散乗算部” 1205-j-a へ出力する。分散逆元計算部 1203-j-a へ入力される値を A_j とし、この入力 A_j と他

のメンバの分散逆元計算部 1203-p-a へ入力される A_p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) の、 t 個の値 A_p ($p=1, 2, \dots, t$) を分散情報として再構成されるようなもとの秘密 A とすると、分散逆元計算部 1203-j-a は、 A の有限体 $GF(q)$ 上の逆元 $B=A^{-1}$ の、仮メンバ ID が d_j であるメンバに対する分散情報 B_j を計算することとなる。分散逆元計算部 1203-j-a は、他のメンバの分散逆元計算部 1203-p-a ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) と秘密通信路 303 を経由して必要な情報をやり取りする。

【0089】

“(2) 分散乗算部” 1205-j-a, 1206-j-a は、内部的には同じ構成であり、2 個の入力を受け取り、それらの入力と秘密通信路 303 からの情報を用いて、2 個の要素の分散乗算を行い、その計算結果を出力する。“(2) 分散乗算部” 1205-j-a, 1206-j-a へ入力される値を $A_{1,j}$, $A_{2,j}$ とする。 $A_{i,j}$ ($i=1, 2$) と、他のメンバの“(2) 分散乗算部” 1205-p-a, 1206-p-a へ入力される $A_{i,p}$ ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) の、2 個の値 $A_{i,p}$ ($p=1, 2, \dots, t$) を分散情報として再構成されるようなもとの秘密を A_i ($i=1, 2$) とすると、“(2) 分散乗算部” 1205-j-a, 1206-j-a は、 A_1 及び A_2 を乗算した値 $B=A_1 \times A_2$ の、仮メンバ ID が d_j であるメンバに対する分散情報 B_j を計算することとなる。“(2) 分散乗算部” 1205-j-a は、“(t-1) 分散乗算部” 1204-j-a 及び分散逆元計算部 1203-j-a からの出力を受け取り、それらを用いて計算し、その計算結果を“(2) 分散乗算部” 1206-j-a へ出力する。“(2) 分散乗算部” 1205-j-a は、他のメンバの“(2) 分散乗算部” 1205-p-a ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) と秘密通信路 303 を経由して必要な情報をやり取りする。“(2) 分散乗算部” 1206-j-a は、“(2) 分散乗算部” 1205-j-a からの出力、及び、項計算部 1101-j-a へ入力される $X_{m,a,j}$ を受け取り、それらを用いて計算し、その計算結果を出力する。“(2) 分散乗算部” 1206-j-a は、他のメンバの“(2) 分散乗算部” 1206

— $p - a$ ($p = 1, 2, \dots, t$ であり、 $p \neq j$ であるもの) と秘密通信路 303 を経由して必要な情報をやり取りする。

【0090】

図16は、図15の“(2)分散乗算部”1205-j-a, 1206-j-a ($j = 1, 2, \dots, t$, $a = 1, 2, \dots, t$) の構成を示すブロック図である。図16を用いて“(2)分散乗算部”1205-j-a, 1206-j-a ($j = 1, 2, \dots, t$, $a = 1, 2, \dots, t$) の構成を説明する。ここで、“(2)分散乗算部”1205-j-a, 1206-j-aへ入力される2つの入力をそれぞれ、 $A d_j$ 及び $B d_j$ とし、“(2)分散乗算部”1205-j-a, 1206-j-aからの出力を $C d_j$ とする。“(2)分散乗算部”1205-j-a, 1206-j-aは、乗算部1301-jと、秘密分散計算部1302-jと、線形結合計算部1303-jとを有する。“(2)分散乗算部”1205-j-a, 1206-j-aへ入力される $A d_j$ 及び $B d_j$ は、乗算部1301-jへ入力され、乗算部1301-jからの出力は、秘密分散計算部1302-jへ入力され、さらに、秘密分散計算部1302-jからの出力は、線形結合計算部1303-jへ入力される。線形結合計算部1303-jからの出力が、“(2)分散乗算部”1205-j-a, 1206-j-aからの出力となる。

【0091】

乗算部1301-jは、“(2)分散乗算部”1205-j-a, 1206-j-aへ入力される $A d_j$ 及び $B d_j$ を受け取り、それらを乗算する。すなわち

$$C' d_j = A d_j \times B d_j \quad \dots (34)$$

を計算して、その計算結果 $C' d_j$ を、秘密分散計算部1302-jへ出力する。

【0092】

秘密分散計算部1302-jは、第2の実施形態における図9の秘密分散計算部701-jと内部的には同じ構成であり、入力される値を (k', t) しきい値秘密分散法を用いて分散して出力する。前述の通り、第3の実施形態の場合、分散乗算を行わなければならないので、この秘密分散法のしきい値 k' は、

$$k' \leq (t+1) / 2 \quad \dots (29)$$

を満たさなければならない。ここで、式(29)の演算は、有限体GF(q)上の演算ではなく、通常の実数、整数演算である。

【0093】

また、分散に用いるときのメンバID $_m'1, m'2, \dots, m't$ は非公開なので、第3の実施形態においては、仮メンバID $_d1, d2, \dots, dt$ を用いる。今、秘密分散計算部1302-jへ入力される値は $C'd_j$ なので、次式(35)の $k'-1$ 次多項式を作り、 $R3d_{j,1}, R3d_{j,2}, \dots, R3d_{j,k'-1}$ は、乱数として有限体GF(q)上の値を $k'-1$ 個選ぶ。

【数18】

$$f_3d_j(x) = C'd_j + R_3d_{j,1}x + R_3d_{j,2}x^2 + \dots + R_3d_{j,k'-1}x^{k'-1} \quad (35)$$

【0094】

仮メンバIDが d_p ($p=1, 2, \dots, t$)であるメンバに対して配布する分散情報 $C'd_{j,p}$ を、上記式(35)を用いて次式(36)のように計算する。

【数19】

$$\begin{aligned} C'd_{j,p} &= f_3d_j(d_p) \\ &= C'd_j + R_3d_{j,1}(d_p) + R_3d_{j,2}(d_p)^2 + \dots + R_3d_{j,k'-1}(d_p)^{k'-1} \end{aligned} \quad (36)$$

【0095】

自分自身に対する分散情報 $C'd_{j,j}$ は、線形結合計算部1303-jへ出力し、その他の分散情報 $C'd_{j,p}$ ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの)を秘密通信路303を通して各メンバに配布する(他のメンバの線形結合計算部1303-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの)へ送信する)。

【0096】

線形結合計算部1303-jは、第2の実施形態における図9の線形結合計算部702-jと内部的には同じ構成であるが、計算に用いるメンバID $_m'1$

, m'_2, \dots, m'_t は非公開なので、第 3 の実施形態においては、仮メンバー ID d_1, d_2, \dots, d_t を用いる。線形結合計算部 1303-j は、秘密分散計算部 1302-j から、分散情報 $C'd_j, j$ を受け取る。さらに、秘密通信路 303 を経由して、他のメンバーの秘密分散計算部 1302-i ($i=1, 2, \dots, t$ で $i \neq j$ であるもの) から配布された分散情報 $C'd_1, j, C'd_2, j, \dots, C'd_t, j$ を受け取る。線形結合計算部 1303-j は、これら全部で t 個ある分散情報 $C'd_p, j$ ($p=1, 2, \dots, t$)、から、次式 (37) 及び (38) のような計算を行い、出力となる Cd_j を算出する。

【数 20】

$$\begin{aligned} Cd_j &= rd_1 C'd_{1,j} + rd_2 C'd_{2,j} + \dots + rd_t C'd_{t,j} \\ &= \sum_{p=1}^t rd_p C'd_{p,j} \quad (37) \end{aligned}$$

$$\begin{aligned} rd_p &= (d_1 \times d_2 \times \dots \times d_t / d_p) \\ &\quad / ((d_1 - d_p) \times (d_2 - d_p) \times \dots \times (d_{p-1} - d_p) \times (d_{p+1} - d_p) \times \dots \times (d_t - d_p)) \\ &= \prod_{\substack{i=1 \\ i \neq p}}^t d_i / (d_i - d_p) \quad (38) \end{aligned}$$

各仮メンバー ID d_1, d_2, \dots, d_t は公開され、既知の値であるので式 (38) の rd_p を計算することができる。

【0097】

図 17 は、図 15 の“(t-1)分散乗算部”1202-j-a, 1204-j-a ($j=1, 2, \dots, t$; $a=1, 2, \dots, t$) の構成を示すブロック図である。図 17 を用いて“(t-1)分散乗算部”1202-j-a, 1204-j-a ($j=1, 2, \dots, t$; $a=1, 2, \dots, t$) の構成を説明する。今、“(t-1)分散乗算部”1202-j-a, 1204-j-a へ入力される $t-1$ 個の入力を A_1, A_2, \dots, A_{t-1} とする。“(t-1)分散乗算部”1202-j-a, 1204-j-a は、 $t-2$ 個の“(2)分散乗算部”1401-i ($i=1, 2, \dots, t-2$) を有する。 $t-2$ 個の“(2)分散乗算部”1401-i ($i=1, 2, \dots, t-2$) は、“(2)分散乗算部”1401-i からの出力が次の“(2)分散乗算部”1401-(i+1) への入力の一つとなるように、多段に構成されている。“(t-1)分散乗算部”1202-j-

$a, 1204-j-a$ へ入力される2つの入力 A_1 及び A_2 は、“(2)分散乗算部”1401-1へ入力され、“(2)分散乗算部”1401-1からの出力は、次の“(2)分散乗算部”1401-2へ、“(t-1)分散乗算部”1202-j-a, 1204-j-aへ入力される A_3 とともに、入力される。“(2)分散乗算部”1401-i ($i=2, \dots, t-2$)へは、“(2)分散乗算部”1401-(i-1)からの出力が、“(t-1)分散乗算部”1202-j-a, 1204-j-aへ入力される $A_{(i+1)}$ とともに、入力され、“(2)分散乗算部”1401-i ($i=1, \dots, t-3$)からの出力は、“(2)分散乗算部”1401-(i+1)に入力される。“(2)分散乗算部”1401-(t-2)からの出力が、“(t-1)分散乗算部”1202-j-a, 1204-j-aからの出力となる。

【0098】

“(2)分散乗算部”1401-i ($i=1, 2, \dots, t-2$)は、前に説明した、“(2)分散乗算部”1205-j-a, 1206-j-aと同じ構成をしている。“(2)分散乗算部”1401-i ($i=1, 2, \dots, t-2$)は、他のメンバの“(2)分散乗算部”1401-i ($i=1, 2, \dots, t-2$)とそれぞれ秘密通信路303を通して通信を行う。

【0099】

図18は、図15の分散逆元計算部1203-j-a ($j=1, 2, \dots, t, a=1, 2, \dots, t$)の構成を示すブロック図である。図18を用いて分散逆元計算部1203-j-a ($j=1, 2, \dots, t, a=1, 2, \dots, t$)の構成を説明する。分散逆元計算部1203-j-aは、 q_b-1 個の“(2)分散乗算部”1501-i ($i=1, 2, \dots, q_b-1$)と、乗算制御部1502と、“(q_b)分散乗算部”1503とを有する。 q_b は、第3の実施形態において前提としている有限体 $GF(q)$ の要素数 q から2を引いた値の底2における対数をとった値(小数点以下切り上げ)であり、次式(39)のように計算できる。

$$q_b = \text{ceil}(\log_2(q-2)) \quad \dots (39)$$

【0100】

ここで、 $\text{ceil}(\cdot)$ は、小数点以下切り上げの演算を表し、 $\log_2(\cdot)$

）は、底 2 の対数をとることを表す。上記式 (39) の演算は、有限体 $GF(q)$ 上の演算ではなく、通常の実数、整数演算である。今、分散逆元計算部 1203-j-a への入力を A_j とすると、この入力 A_j と他のメンバの分散逆元計算部 1203-p-a へ入力される A_p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) の、 t 個の値 A_p ($p=1, 2, \dots, t$) を分散情報としてを再構成されるようなもとの秘密 A とする。この場合、分散逆元計算部 1203-j-a は、 A の有限体 $GF(q)$ 上の逆元 $B=A^{-1}$ の、仮メンバ ID が d_j であるメンバに対する分散情報 B_j を計算して出力することとなる。有限体の性質により、有限体 $GF(q)$ 上の演算においては、有限体 $GF(q)$ のある要素 A に対して、次式 (40)、すなわち、

$$A^{-1} = A^{q-2} \quad \dots (40)$$

が成立するので、分散逆元計算部 1203-j-a においては、 A_j を $q-2$ 回分散乗算する計算を行う。

【0101】

q_b-1 個の“(2)分散乗算部” 1501-i ($i=1, 2, \dots, q_b-1$) は、“(2)分散乗算部” 1501-i からの出力が次の“(2)分散乗算部” 1501-(i+1) への両方の入力となっているように、多段に構成されている。分散逆元計算部 1203-j-a へ入力される入力 A_j は、“(2)分散乗算部” 1501-1 へ入力され、“(2)分散乗算部” 1501-1 からの出力は、次の“(2)分散乗算部” 1501-2 へ入力される。分散逆元計算部 1203-j-a へ入力される入力 A_j 、及び各“(2)分散乗算部” 1501-i ($i=1, 2, \dots, q_b-1$) からの出力の、合計 q_b 個の値は、乗算制御部 1502 へ入力され、乗算制御部 1502 から出力される値は、“(q_b)分散乗算部” 1503 へ入力される。“(q_b)分散乗算部” 1503 からの出力が分散逆元計算部 1203-j-a からの出力となる。

【0102】

“(2)分散乗算部” 1501-i ($i=1, 2, \dots, q_b-1$) は、前に説明した、“(2)分散乗算部” 1205-j-a, 1206-j-a と同じ構成をしている。“(2)分散乗算部” 1501-i ($i=1, 2, \dots, q_b-1$)

は、他のメンバの“(2)分散乗算部” $1501-i$ ($i=1, 2, \dots, q_b-1$) とそれぞれ秘密通信路303を通して通信を行う。

【0103】

乗算制御部1502は、分散逆元計算部 $1203-j-a$ へ入力される入力 A_j 及び各“(2)分散乗算部” $1501-i$ ($i=1, 2, \dots, q_b-1$) からの出力の、合計 q_b 個の値を受け取り、入力された q_b 個の値を、そのまま出力するか、又は、1を出力する、ということを制御する。入力されたそれぞれの値をどう出力するかは、次のようなルールで行う。まず、“(2)分散乗算部” $1501-i$ ($i=1, 2, \dots, q_b-1$) からの出力を $A_{j,i+1}$ とする。乗算制御部1502へは、 q_b 個の値 $A_{j,i}$ ($i=1, 2, \dots, q_b$) が入力されることとなる(ただし、 $A_{j,1}=A_j$)。また、 $q-2$ を2進数表現し、そのときの各桁の値を大きい桁から $b_{q_b}, b_{(q_b-1)}, \dots, b_2, b_1$ とする($q-2$ は、 q_b 桁の2進数で表すことができる)。乗算制御部1502は、上記 b_i ($i=1, 2, \dots, q_b$) が1であるならば値 $A_{j,i}$ を出力し、上記 b_i ($i=1, 2, \dots, q_b$) が0であるならば値1を出力する。出力された q_b 個の値は、“(q_b)分散乗算部”1503へ入力される。

【0104】

“(q_b)分散乗算部”1503は、前述した“($t-1$)分散乗算部” $1202-j-a, 1204-j-a$ と同様な構成をしているが、“(2)分散乗算部”が $t-2$ 個ではなく、 q_b-1 個になっている構成である。“(q_b)分散乗算部”1503は、他のメンバの“(q_b)分散乗算部”1503とそれぞれ秘密通信路303を通して通信を行う。

【0105】

[第3の実施形態の動作]

図19は、第3の実施形態に係る秘密再構成方法における動作を示すフローチャートである。ここで、もとの秘密情報 S を再構成するために集まった t 人のメンバのメンバIDを m'_1, m'_2, \dots, m'_t とし、各メンバが持つ分散情報を $X_{m'_1}, X_{m'_2}, \dots, X_{m'_t}$ とする。

【0106】

図19に示されるように、まず、集まった各メンバに対して、分散計算時に用いる仮メンバIDを割り当てるために、仮メンバID $_d_1, d_2, \dots, d_t$ を生成し、各メンバに配布、そして、公開する（ステップS1601）。ステップS1601は、図12の仮メンバID生成部901における動作を示しており、各メンバに重複なく仮メンバID $_d_1, d_2, \dots, d_t$ を割り当て、配布、公開する。

【0107】

次に、各メンバが持つ分散情報及びメンバIDを (k', t) しきい値秘密分散法を用いて分散し、他のメンバに配布する（ステップS1602）。ステップS1602は、図13の秘密分散計算部1001-jにおける動作を示しており、メンバIDが m'_j ($j=1, 2, \dots, t$)であるメンバの持つ分散情報 $X_{m'_j}$ を上記式(29')を用いて分散して、仮メンバIDが d_p ($p=1, 2, \dots, t$)であるメンバに対し、上記式(30)で計算される $X_{m'_j, p}$ を配布し、メンバID $_m'_j$ を上記式(31)を用いて分散して、仮メンバIDが d_p ($p=1, 2, \dots, t$)であるメンバに対し、上記式(32)で計算される $m'_{j, p}$ を配布する。

【0108】

次に、各メンバは、公開されている集まったメンバの仮メンバID、自分自身の分散情報及びメンバIDのそれぞれの分散情報、及び、他のメンバから配布された分散情報及びメンバIDのそれぞれの分散情報を用いて演算を施し、もとの秘密情報Sの分散情報である値を求める（ステップS1603）。ステップS1603は、図13の分散処理部1002-jにおける動作を示しており、秘密再構成するための演算（上記式(3)）を、メンバID $_m'_j$ ($j=1, 2, \dots, t$)及び分散情報 $X_{m'_j}$ を秘密にしたまま、上記式(3)の分散計算を行い、最終的に、仮メンバIDが d_j ($j=1, 2, \dots, t$)であるメンバは、再構成すればもとの秘密情報Sとなるような分散秘密情報 S_{d_j} を得る。

【0109】

次に、ステップS1603で、各メンバが計算した分散情報及び仮メンバIDからもとの秘密情報Sを再構成する（ステップS1604）。ステップS160

4 は、図 12 の秘密再構成計算部 903 における動作を示しており、仮メンバ ID が d_j ($j = 1, 2, \dots, t$) であるメンバがステップ S1603 で計算した結果 S_{d_j} ($j = 1, 2, \dots, t$)、及び仮メンバ ID $_d_j$ ($j = 1, 2, \dots, t$) から、上記式 (27) を用いて計算し、もとの秘密情報 S を得ることができる。

【0110】

[第3の実施形態の効果]

以上説明したように、第3の実施形態によれば、上記第1及び第2の実施形態と同様に、もとの秘密情報 S を再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報 S を再構成することができる。したがって、各メンバが持つ分散情報を、次の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを必要とせずに、上記の効果を達成することができる。

【0111】

また、第3の実施形態においては、第1の実施形態とは異なり、 (k, n) しきい値秘密分散法を用いているので、必ずしもメンバ全員、すなわち n 人が集まらなくとも、 k 人 ($k \leq n$) 以上が集まれば、もとの秘密情報 S を再構成することができる。

【0112】

さらに、第3の実施形態においては、第2の実施形態とは異なり、各メンバが保有する分散情報だけでなく、メンバ ID をも公開せずに秘密情報の再構成を行なう。したがって、集まったメンバの匿名性を確保することができる。

【0113】

さらに、第3の実施形態においては、第1及び第2の実施形態と同様に、予め秘密情報 S の分散情報を持たない人（演算記憶装置）が、この再構成に参加しようとしても、もとの秘密情報 S の再構成に失敗することから、第3の実施形態においては、集まった複数人数からなるグループ全員が正当メンバ（予め秘密情報 S の分散情報を配布されたメンバ）か、そうでない人（演算記憶装置）が混在するか、ということを認証するような機能が、効果として備わる。さらに、前述の

ように再利用可能なので、この認証機能は、秘密情報 S の分散情報を更新せずとも何度も利用できる。また、この認証機能は、集まったメンバから他へ送信される情報は、認証（もとの秘密情報 S の再構成）のたびに異なるので、盗聴によるなりすましに非常に強い。特に、第 3 の実施形態においては、前述のように、「[1] もとの秘密情報 S の分散情報を持つメンバの全員が集まらなくとも、しきい値以上のメンバが集まればよい。[2] 匿名性がある。」という 2 つの効果があることから、集まった複数人数からなるグループ全員が正当メンバであると認証された場合でも、どのメンバが集まっているかを具体的に特定せずに認証が可能である。このような認証機能は、秘密分散法の秘密再構成の性質と、マルチパーティ・プロトコルによる分散計算の性質との単なる組み合わせによって得られる機能ではなく、新しい機能である。ただし、第 1、第 2 の実施形態の効果で説明したと同様に、上記認証機能は、「もとの秘密情報 S 」を照合秘密情報 S （予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いる利用形態であるので、もとの秘密情報 S を各メンバに秘密にしない場合であっても、実現できる。

【0114】

《第 4 の実施形態》

[第 4 の実施形態の概要]

上記第 3 の実施形態においては、もとの秘密情報 S を再構成する際に用いるマルチパーティ・プロトコルは、計算するために集まったメンバのうち、どの 2 人のメンバ間にも、その 2 人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されていることを前提とする方式（前述したマルチパーティ・プロトコルの第 1 方式）であったが、第 4 の実施形態においては、計算するために集まったメンバ間の通信には、上記秘密通信路を用いる通信手法に加え、紛失通信と呼ばれる通信手法を用いる方式（前述したマルチパーティ・プロトコルの第 2 方式）を用いる。これにより、第 4 の実施形態に係る秘密再構成方法によれば、第 3 の実施形態に係る秘密再構成方法による効果と同様の効果を得ることができる。さらに、第 4 の実施形態に係る秘密再構成方法によれば、上記第 3 の実施形態に係る秘密再構成方法における分散計算に用いる (k', t) しきい値秘

密分散法のしきい値 k' の制限、すなわち、次式 (29) の制限、

$$k' \leq (t+1)/2 \quad \dots (29)$$

を取り払い、しきい値 k' のとり得る範囲を、 $k' \leq t$ まで広げることができる。

【0115】

[第4の実施形態の構成]

第4の実施形態に係る秘密再構成方法を実施する構成（第4の実施形態に係る秘密再構成システム）は、上記第3の実施形態に係る秘密再構成方法を実施する構成とほぼ同じであるが、前述したマルチパーティ・プロトコルの第2方式を用いているので、図16の“(2)分散乗算部”1205-j-a, 1206-j-aの構成のみが異なる。第4の実施形態の説明においては、上記第3の実施形態に係る秘密再構成方法を実施する構成と異なる部分、すなわち、“(2)分散乗算部”1205-j-a, 1206-j-aの構成のみを説明する。

【0116】

図20は、本発明の第4の実施形態に係る秘密再構成方法で使用される“(2)分散乗算部”1205-j-a, 1206-j-aの構成を示すブロック図である。第4の実施形態においては、“(2)分散乗算部”1205-j-a, 1206-j-aを、図20に示されるように構成することによって、上記第3の実施形態における制限である、上記式(29)の制限を取り払うことができる。このため、しきい値 k' のとり得る範囲を、 $k' \leq t$ まで広げることができる。図20の構成は、前述したマルチパーティ・プロトコルの第2方式を利用している。

【0117】

次に、図20を用いて、第4の実施形態における、“(2)分散乗算部”1205-j-a, 1206-j-aの構成を説明する。図20に示されるように、第4の実施形態における“(2)分散乗算部”1205-j-a, 1206-j-aは、jj項計算部1701-jと、ij項計算部1702-jと、“(t)加算部”1703-jとを有している。“(2)分散乗算部”1205-j-a, 1206-j-aに入力される2つの入力 A_{dj} , B_{dj} は、jj項計算部1701-jと、ij項計算部1702-jとの両方に入力される。jj項計算部

1701-jからの出力及びij項計算部1702-jからの出力は、“(t)加算部”1703-jに入力される。“(t)加算部”1703-jからの出力が、“(2)分散乗算部”1205-j-a, 1206-j-aの出力となる。

【0118】

jj項計算部1701-jは、“(2)分散乗算部”1205-j-a, 1206-j-aに入力される2つの入力 $A d_j$, $B d_j$ を受け取り、それらを乗算し、次式(41)で計算される係数 $r d_j$ をさらに乗算して、“(t)加算部”1703-jに出力する。

【数21】

$$\begin{aligned} r d_j &= (d_1 \times d_2 \times \cdots \times d_t / d_j) \\ &\quad / ((d_1 - d_j) \times (d_2 - d_j) \times \cdots \times (d_{j-1} - d_j) \times (d_{j+1} - d_j) \times \cdots \times (d_t - d_j)) \\ &= \prod_{\substack{i=1 \\ i \neq j}}^t d_i / (d_i - d_j) \quad (41) \end{aligned}$$

【0119】

詳細に言えば、jj項計算部1701-jは、 $A d_j \times B d_j$ を計算し、上記式(41)の係数 $r d_j$ をさらに掛けた $r d_j (A d_j \times B d_j)$ を計算して、出力する。

【0120】

ij項計算部1702-jは、“(2)分散乗算部”1205-j-a, 1206-j-aに入力される2つの入力 $A d_j$, $B d_j$ を受け取り、受け取った入力 $A d_j$, $B d_j$ と秘密通信路303を通して他のメンバから受け取った情報から、実質的に他のメンバの値との乗算結果が得られるように計算をする。例えば、仮メンバIDが d_j であるメンバは、“(2)分散乗算部”1205-j-a, 1206-j-aに入力される $A d_j$ と $B d_j$ の乗算 $A d_j \times B d_j$ をjj項計算部1701-jで行うが、ij項計算部1702-jにおいては、他のメンバ(メンバIDが d_p であり、 $p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの)の値との乗算、 $A d_j \times B d_p$ 及び $A d_p \times B d_j$ の結果に相当するもの(乗算結果そのものではない)が得られるようにする。

【0121】

i, j 項計算部 1702-j は、

$$A d_j \times B d_p = D d_j + D d_p \quad \cdots (42)$$

$$A d_p \times B d_j = E d_j + E d_p \quad \cdots (42')$$

となるような、 $D d_j$ 及び $E d_j$ を仮メンバ ID が d_j であるメンバが持つことができ、 $D d_p$ 及び $E d_p$ を仮メンバ ID が d_p であるメンバが持つことができるように、計算を行う。

【0122】

図 21 は、図 20 の i, j 項計算部 1702-j の構成を示すブロック図である。図 21 を用いて、 i, j 項計算部 1702-j の構成を説明する。図 21 に示されるように、 i, j 項計算部 1702-j は、 $j-1$ 個の項計算受信部 1801-j-p ($p=1, 2, \dots, j-1$) と、 $j-1$ 個の項計算受信部 1802-j-p ($p=1, 2, \dots, j-1$) と、 $t-j$ 個の項計算送信部 1803-j-p, ($p=j+1, j+2, \dots, t$) と、 $t-j$ 個の項計算送信部 1804-j-p ($p=j+1, j+2, \dots, t$) と、 $t-1$ 個の加算部 1805-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) と、 $t-1$ 個の係数乗算部 1806-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) とを有している。

【0123】

i, j 項計算部 1702-j へ入力される 2 つの入力のうち、一つは、項計算受信部 1801-j-p ($p=1, 2, \dots, j-1$) 及び項計算送信部 1803-j-p ($p=j+1, j+2, \dots, t$) へ、他の一つは、項計算受信部 1802-j-p ($p=1, 2, \dots, j-1$) 及び項計算送信部 1804-j-p ($p=j+1, j+2, \dots, t$) へ入力される。項計算受信部 1801-j-p 及び項計算受信部 1802-j-p ($p=1, 2, \dots, j-1$) からの出力は、加算部 1805-j-p ($p=1, 2, \dots, j-1$) へ入力され、項計算送信部 1803-j-p 及び項計算送信部 1804-j-p ($p=j+1, j+2, \dots, t$) からの出力は、加算部 1805-j-p ($p=j+1, j+2, \dots, t$) へ入力される。加算部 1805-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) からの出力は係数乗算部 1806-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) へ入力される。

【0124】

係数乗算部 1806-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) からの出力 (全部で $t-1$ 個の出力) が、ij 項計算部 1702-j からの出力となる。項計算受信部 1801-j-p, 1802-j-p ($p=1, 2, \dots, j-1$)、及び項計算送信部 1803-j-p, 1804-j-p ($p=j+1, j+2, \dots, t$) は、秘密通信路 303 を通して、他のメンバとの情報のやりとりを行うことにより、前述の通り、他のメンバ (メンバ ID が d_p であり、 $p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) の値との乗算、 $A d_j \times B d_p$ 及び $A d_p \times B d_j$ の結果に相当するもの (乗算結果そのものではない) が得られるようにするが、他のメンバの値 $A d_p$ 及び $B d_p$ (メンバ ID が d_p であり、 $p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) が分からないように、また、自分の値 $A d_j$ 及び $B d_j$ が、他のメンバに分からないように、紛失通信を行う。紛失通信とは、ここでは、送信側が、M 個の情報を符号化 (暗号化) して送信するが、受信側においては、そのうち一つしか受け取る (意味のあるように復号が可能となる) ことができず、また、送信側においては、受信側がどの情報を受け取った (意味のあるように復号が可能となった) かを知ることができない通信方法をいう。この実施形態においては、法 q のもとにおける離散対数を計算することが困難であることを利用して、紛失通信を構成する。

【0125】

項計算受信部 1801-j-p, 1802-j-p ($p=1, 2, \dots, j-1$)、及び項計算送信部 1803-j-p, 1804-j-p ($p=j+1, j+2, \dots, t$) は、 j の値によって、項計算受信部又は項計算送信部を持つ場合と、持たない場合とがある。例えば、 $j=1$ の場合には、項計算受信部を持たず、 $2 \times (t-1)$ 個の項計算送信部を持つ。また、 $j=t$ の場合には、項計算送信部を持たず、 $2 \times (t-1)$ 個の項計算受信部を持つ。また、他のメンバとの送受信の関係は、仮メンバ ID が d_j であるメンバの項計算送信部 1803-j-p, 1804-j-p ($p=j+1, j+2, \dots, t$) からは、それぞれ、秘密通信路 303 を通して、仮メンバ ID が d_p であるメンバの項計算受信部 1801-p-j, 1802-p-j のそれぞれへ情報が渡される。これについては、

図 2 2 及び図 2 3 で説明する。

【0126】

加算部 1805-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) は、項計算受信部 1801-j-p, 1802-j-p ($p=1, 2, \dots, j-1$)、又は項計算送信部 1803-j-p, 1804-j-p ($p=j+1, j+2, \dots, t$) からの出力を受け取り、それらを加算して、係数乗算部 1806-j-p ($p=1, 2, \dots, t$ であり、 $a \neq j$ であるもの) へ出力する。項計算受信部 1801-j-p 又は項計算送信部 1803-j-p からの出力を $Dd_{j,p}$ とし、項計算受信部 1802-j-p 又は項計算送信部 1804-j-p からの出力を $Ed_{j,p}$ とすると、加算部 1805-j-p においては、 $Dd_{j,p} + Ed_{j,p}$ を計算して、その計算結果を係数乗算部 1806-j-p へ出力する。

【0127】

係数乗算部 1806-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) は、加算部 1805-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) からの出力を受け取り、次式 (43) で計算される係数を乗算して出力する。

【数 2 2】

$$\begin{aligned} rd_p &= (d_1 \times d_2 \times \dots \times d_t / d_p) \\ &\quad / ((d_1 - d_p) \times (d_2 - d_p) \times \dots \times (d_{p-1} - d_p) \times (d_{p+1} - d_p) \times \dots \times (d_t - d_p)) \\ &= \prod_{\substack{i=1 \\ i \neq p}}^t d_i / (d_i - d_p) \quad (43) \end{aligned}$$

【0128】

加算部 1805-j-p からの出力を $Fd_{j,p}$ とすると、係数乗算部 1806-j-p は、 $rd_p \times Fd_{j,p}$ を計算して、その計算結果を出力する。係数乗算部 1806-j-p ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) からの出力 (全部で $t-1$ 個の出力) が、ij 項計算部 1702-j からの出力となる。

【0129】

次に、図 2 2 を用いて、項計算受信部 1801-j-p, 1802-j-p (

$p = 1, 2, \dots, j-1$) の構成を説明する。項計算受信部 1801-j-p, 1802-j-p ($p = 1, 2, \dots, j-1$) は、インデックス計算送信部 1901-j 及び受信復元部 1902-j からなる。項計算受信部 1801-j-p は、 i, j 項計算部 1702-j の 2つの入力のうち一つの入力を受け取り、項計算受信部 1802-j-p は、他の一つの入力を受け取る。ここでは、項計算受信部 1801-j-p への入力を A_{dj} 、項計算受信部 1802-j-p への入力を B_{dj} とおく。項計算受信部 1801-j-p と 1802-j-p は、内部的に同じ構造なので、ここでは、項計算受信部 1801-j-p について説明し、項計算受信部 1802-j-p に相当する説明は、括弧 [] の中に記述する。項計算受信部 1801-j-p [1802-j-p] への入力、インデックス計算送信部 1901-j へ入力される。インデックス計算送信部 1901-j からの出力は、受信復元部 1902-j へ入力される。受信復元部 1902-j からの出力が項計算受信部 1801-j-p [1802-j-p] からの出力となる。

【0130】

インデックス計算送信部 1901-j は、項計算受信部 1801-j-p [1802-j-p] への入力 A_{dj} [B_{dj}] を受け取り、次式 (44) 及び (44') で示す計算を施して、 $A'_{dj,p}$ [$B'_{dj,p}$] を計算し、秘密通信路 303 を通して、仮メンバ ID が d_p であるメンバへ送信する ($p = 1, 2, \dots, j-1$)。

【数 23】

$$A'_{dj,p} = g^{r_{Aj,p}} h^{A_{dj}} \quad (44)$$

$$B'_{dj,p} = g^{r_{Bj,p}} h^{B_{dj}} \quad (44')$$

【0131】

上記式 (44) 及び (44') において、 h 及び g は、有限体 $GF(q)$ 上の 2つの生成元とし、 $r_{Aj,p}$ [$r_{Bj,p}$] は、乱数として有限体 $GF(q)$ 上の値を選ぶ。また、インデックス計算送信部 1901-j は、上記式 (44) [(44')] で用いた乱数 $r_{Aj,p}$ [$r_{Bj,p}$] を受信復元部 1901

— j へ出力する。

【0132】

受信復元部 1901-j は、仮メンバ ID が d_p ($p = 1, 2, \dots, j-1$) であるメンバから q 個 (q は有限体 $GF(q)$ の要素数) の情報を受け取り、 A_{d_j} 番目の情報 $D'_{d_j, p}$ [B_{d_j} 番目の情報 $E'_{d_j, p}$] を用いて、次式 (45) 及び (45') で計算することにより、目的とする値 $D_{d_j, p}$ [$E_{d_j, p}$] を計算する (それ以外の受け取った情報は、仮メンバ ID が d_j であるメンバにとっては、乱数に見える)。 $D'_{d_j, p}$ [$E'_{d_j, p}$] は、2つの情報、 $D'_{1, d_j, p}$ 及び $D'_{2, d_j, p}$ [$E'_{1, d_j, p}$ 及び $E'_{2, d_j, p}$] から成っているものとする。

【数24】

$$D_{d_j, p} = D'_{1, d_j, p} / ((D'_{2, d_j, p})^{r_{A_{d_j, p}}}) \quad (45)$$

$$E_{d_j, p} = E'_{1, d_j, p} / ((E'_{2, d_j, p})^{r_{B_{d_j, p}}}) \quad (45')$$

上記式 (45) 及び (45') で計算される $D_{d_j, p}$ [$E_{d_j, p}$] が、受信復元部 1902-j の出力となり、項計算受信部 1801-j-p [$1802-j-p$] からの出力となる。

【0133】

次に、図 23 を用いて、項計算送信部 1803-j-p, 1804-j-p ($p = j+1, j+2, \dots, t$) の構成を説明する。図 23 に示されるように、項計算送信部 1803-j-p, 1804-j-p ($p = j+1, j+2, \dots, t$) は、乱数生成部 2001-j と、有限体要素生成部 2002-j と、乗数計算送信部 2003-j-a ($a = 1, 2, \dots, q$) とを有している。項計算送信部 1803-j-p, 1804-j-p ($p = j+1, j+2, \dots, t$) への入力 は、乱数生成部 2001-j 及び有限体要素生成部 2002-j からの出力とともに、乗数計算送信部 2003-j-a ($a = 1, 2, \dots, q$) へ入力される。乱数生成部 2001-j からの出力が、項計算送信部 1803-j-p, 1804-j-p ($p = j+1, j+2, \dots, t$) からの出力となる。項計算送信部 1803-j-p は、 i_j 項計算部 1702-j の 2つの入力のうち一つの入力を

受け取り、項計算送信部 1804-j-p は、他の一つの入力を受け取る。ここでは、項計算送信部 1803-j-p への入力を Ad_j 、項計算送信部 1804-j-p への入力を Bd_j とおく。項計算送信部 1803-j-p と 1804-j-p は、内部的に同じ構造なので、ここでは、項計算送信部 1803-j-p について説明し、項計算送信部 1804-j-p に相当する説明は、括弧 [] の中に記述する。

【0134】

乱数生成部 2001-j は、有限体 $GF(q)$ 上の値の乱数を生成して出力する。乗数計算送信部 2003-j-a ($a=1, 2, \dots, q$) へは、同じ乱数が出力される。乱数生成部 2001-j からの出力が項計算送信部 1803-j-p [1804-j-p] ($p=j+1, j+2, \dots, t$) からの出力となる。

【0135】

有限体要素生成部 2002-j は、有限体 $GF(q)$ 上の値を $0, 1, \dots, q-1$ と、順次生成し、それぞれ、乗数計算送信部 2003-j-a ($a=1, 2, \dots, q$) へ出力する。すなわち、乗数計算送信部 2003-j-1 へは 0 を、乗数計算送信部 2003-j-2 へは 1 を、乗数計算送信部 2003-j-i へは $i-1$ を、乗数計算送信部 2003-j-q へは $q-1$ を、出力する。

【0136】

乗数計算送信部 2003-j-a ($a=1, 2, \dots, q$) は、項計算送信部 1803-j-p [1804-j-p] ($p=j+1, j+2, \dots, t$) から入力される値 Ad_j [Bd_j]、乱数生成部 2001-j からの乱数を、有限体要素生成部 2002-j から対応する有限体要素 $a-1$ を、秘密通信路 303 を通して仮メンバ ID が d_p ($p=j+1, j+2, \dots, t$) であるメンバからの情報 (他のメンバの項計算受信部 1801-p-j [1802-p-j] のインデックス計算送信部 1901-p からの出力) $A'd_{p,j}$ [$B'd_{p,j}$] を、受け取り、それらの入力から計算をして、計算結果を出力する。乗数計算送信部 2003-j-a ($a=1, 2, \dots, q$) からの出力、合計 q 個の出力は、秘密通信路 303 を通して、 a の小さい順に、仮メンバ ID が d_p ($p=j+1, j+2, \dots, t$) であるメンバへ送信する。

【0137】

今、乱数生成部2001-jからの出力を $Dd_{j,p}$ [$Ed_{j,p}$] とする。
 また、秘密通信路303を通して受信する値を、 $A'd_{p,j}$ (項計算送信部1803-j-pに相当) [$B'd_{p,j}$ (項計算送信部1804-j-pに相当)] とする。有限体要素生成部2002-jから乗数計算送信部2003-j-a ($a=1, 2, \dots, q$)へは、 $a-1$ が入力される。乗数計算送信部2003-j-a ($a=1, 2, \dots, q$)は、次式(46)、(46')、(47)、(47')、(48)、(48')の計算を行い、 $D'd_{p,j,a}$ [$E'd_{p,j,a}$] をそれぞれ計算し($D'd_{p,j,a}$ [$E'd_{p,j,a}$] は式(45) [式(45')] の説明で述べたように2つの値からなる)、秘密通信路303を通して仮メンバーIDが d_p ($p=j+1, j+2, \dots, t$)であるメンバーへ、 $a=1, 2, \dots, q$ の順に送信する。

【0138】

【数25】

$$D'_1 d_{p,j,a} = g^{kA_a} \quad (46)$$

$$E'_1 d_{p,j,a} = g^{kB_a} \quad (46')$$

$$D'_2 d_{p,j,a} = (Ad_j(a-1) - Dd_{j,p}) (A'd_{p,j}/h^a)^{kA_a} \quad (47)$$

$$E'_2 d_{p,j,a} = (Bd_j(a-1) - Ed_{j,p}) (B'd_{p,j}/h^a)^{kB_a} \quad (47')$$

$$D'd_{p,j,a} = (D'_1 d_{p,j,a}, D'_2 d_{p,j,a}) \quad (48)$$

$$E'd_{p,j,a} = (E'_1 d_{p,j,a}, E'_2 d_{p,j,a}) \quad (48')$$

【0139】

上記式において、 kA_a [kB_a] ($a=1, 2, \dots, q$)は、それぞれ、 q 個の有限体GF(q)上の値の乱数である。これらの出力 $D'd_{p,j,a}$ 又は $E'd_{p,j,a}$ を秘密通信路303を通して、仮メンバーIDが d_p ($p=j+1, j+2, \dots, t$)であるメンバーの項計算受信部1801-p-j [項計算受信部1802-p-j] が受け取ると、受け取ったメンバーは、 $a=Ad_{p,j}$ [$Bd_{p,j}$] に相当する a 番目の情報 $D'd_{p,j}=D'd_{p,j,a}$ [$E'd_{p,j}=E'd_{p,j,a}$] を式(45) [式(45')] で復号することが

できる（それ以外の受け取った情報は、仮メンバIDが d_p であるメンバにとっては、乱数に見える）。

【0140】

このように、図20から図23までに示されるような構成を採用した場合には、“（2）分散乗算部”1205-j-a, 1206-j-aにおける式（29）の制限をなくすことができる（すなわち $k' \leq t$ まで、しきい値 k' の範囲を拡大することができる）。

【0141】

[第4の実施形態の動作]

第4の実施形態に係る秘密再構成方法における動作は、上記第3の実施形態における動作とほぼ同じであり、図19のフローチャートとほぼ同じであるが、図19のステップS1603の動作に、異なる点を持つ。上記第3の実施形態においては、ステップS1603の計算に用いる“（2）分散乗算部”1205-j-a, 1206-j-aは、図16のような構成で計算処理を行っていたが、第4の実施形態においては、図20のような構成で計算処理を行う。

【0142】

[第4の実施形態の効果]

以上説明したように、第4の実施形態によれば、上記第1、第2、第3の実施形態と同様に、もとの秘密情報Sを再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報Sを再構成することができる。したがって、各メンバが持つ分散情報を、次の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを必要とせずに、上記の効果を達成することができる。

【0143】

また、第4の実施形態においては、上記第3の実施形態と同様な効果を得ることができるだけでなく、上記第3の実施形態における、分散計算に用いる（ k' , t ）しきい値秘密分散法のしきい値 k' の制限、

$$k' \leq (t+1)/2 \quad \dots (29)$$

を取り払い、 $k' \leq t$ まで、しきい値 k' のとり得る範囲を広げることができる。

【0144】

《第5の実施形態》

[第5の実施形態の概要]

上記第3の実施形態においては、図15に示される分散逆元計算部1203-j-a ($j=1, 2, \dots, t$ であり、 $a=1, 2, \dots, t$ である。)は、図18に示されるように、 (q_b-1) 個の“(2)分散乗算部”を有している。これに対し、以下に説明する第5の実施形態によれば、分散逆元計算部1203-j-a内に備えられる“(2)分散乗算部”の個数を減らすことができる。

【0145】

分散逆元計算部1203-j-aへ入力される値を A_j とし、この入力 A_j と他のメンバの分散逆元計算部1203-p-aへ入力される A_p ($p=1, 2, \dots, t$ であり、 $p \neq j$ である。)の、 t 個の値 A_p ($p=1, 2, \dots, t$)を分散情報として再構成されるようなもとの秘密情報を A とすると、分散逆元計算部1203-j-aは、もとの秘密情報 A の有限体 $GF(q)$ 上の逆元 $C=A^{-1}$ の、仮メンバIDが d_j であるメンバに対する分散情報 C_j を計算する。第5の実施形態においては、分散逆元計算部1203-j-aへの入力値 A_j ($j=1, 2, \dots, t$)に、各メンバそれぞれが生成した乱数 B_j ($j=1, 2, \dots, t$)を用いて分散乗算することにより、入力値 A_j を隠蔽した上で、その乱数 B_j を分散乗算された値 U_j ($j=1, 2, \dots, t$)を公開し、 U_j を分散情報として再構成されるようなもとの秘密 U を再構成する。もとの秘密情報 U の逆元 U^{-1} を算出し、逆元 U^{-1} の分散情報 U^{-1}_j を各メンバに分散する。各メンバは、その受け取った分散情報 U^{-1}_j と発生させた乱数 B_j から、求める値 $C_j=A^{-1}_j$ を得る。

【0146】

[第5の実施形態の構成]

第5の実施形態の秘密再構成方法を実施する構成(第5の実施形態に係る秘密再構成システム)は、上記第3の実施形態に係る秘密再構成方法を実施する構成とはほぼ同じであるが、図15の分散逆元計算部1203-j-a ($j=1, 2, \dots, t$ であり、 $a=1, 2, \dots, t$ である。)の構成のみが異なる。第5の実施

形態の説明においては、上記第3の実施形態と異なる部分、すなわち、分散逆元計算部 1203-j-a の構成のみを説明する。

【0147】

図24 (a) 及び (b) を用いて、第5の実施形態の分散逆元計算部 1203-j-a ($j=1, 2, \dots, t$ であり、 $a=1, 2, \dots, t$ である。) の構成を説明する。図24 (a) は、集まったメンバのうち、ある代表メンバを一つ決定し (その仮メンバIDを d_j とする)、そのメンバの分散逆元計算部 1203-j-a ($a=1, 2, \dots, t$) の構成を表している。この代表メンバは、どのように決定してもよいが、例えば、仮メンバIDが最小 (又は最大) であるメンバにすると予め決めておくことで可能である。また、図24 (b) は、その代表メンバ以外のメンバ (仮メンバIDを d_i ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) とする) の分散逆元計算部 1203-i-a ($a=1, 2, \dots, t$) の構成を表している。

【0148】

まず、代表メンバの分散逆元計算部 1203-j-a (図24 (a)) を説明する。図24 (a) に示されるように、代表メンバの分散逆元計算部 1203-j-a は、乱数生成部 2101-j と、“(2) 分散乗算部” 2102-j と、2106-j と、線形結合計算部 2103-j と、逆元計算部 2104-j と、秘密分散計算部 2105-j とを有する。分散逆元計算部 1203-j-a への入力 ($A d_j$ とする) は、乱数生成部 2101-j からの出力とともに、“(2) 分散乗算部” 2102-j へ入力される。“(2) 分散乗算部” 2102-j からの出力は、線形結合計算部 2103-j へ入力され、線形結合計算部 2103-j からの出力は、逆元計算部 2104-j へ入力され、さらに、逆元計算部 2104-j からの出力は、秘密分散計算部 2105-j へ入力される。秘密分散計算部 2105-j からの出力は、乱数生成部 2101-j からの出力とともに、“(2) 分散乗算部” 2106-j へ入力される。“(2) 分散乗算部” 2106-j からの出力が、代表メンバの分散逆元計算部 1203-j-a からの出力となる。

【0149】

乱数生成部 2101-j は、有限体 $GF(q)$ 上の値の乱数を生成して出力する。出力先は、“(2) 分散乗算部” 2102-j 及び 2106-j で、両方に同じ乱数を出力する。

【0150】

“(2) 分散乗算部” 2102-j は、分散逆元計算部 1203-j-a への入力 Ad_j 及び乱数生成部 2101-j からの出力を受け取り、それらを入力として、秘密通信路 303 からの情報を用いながら演算を行い、その演算結果を、線形結合計算部 2103-j へ出力する。第 5 の実施形態における“(2) 分散乗算部” 2102-j の構成は、図 16 の“(2) 分散乗算部” 1205-j-a, 1206-j-a の構成、又は、図 20 の“(2) 分散乗算部” 1205-j-a, 1206-j-a の構成と同じである。

【0151】

線形結合計算部 2103-j は、“(2) 分散乗算部” 2102-j の出力結果、及び、秘密通信路 303 を通して他のメンバからの“(2) 分散乗算部” 2102-i (後述する図 24 (b)、 $i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) の出力結果を受け取り、線形結合計算を行い、計算結果を逆元計算部 2104-j へ出力する。第 5 の実施形態における線形結合計算部 2103-j の構成は、図 9 の線形結合計算部 702-j の構成と同様なものである。“(2) 分散乗算部” 2102-j の出力結果を Ud_j とし、秘密通信路 303 を通して他のメンバからの“(2) 分散乗算部” 2102-i (後述する図 24 (b)、 $i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) の出力結果を Ud_i ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) とすると、線形結合計算部 2103-j は、前述した式 (25) 及び (26) と同様な次式 (49) 及び (50) を計算し、その結果 U を逆元計算部 2104-j へ出力する。

【数 2 6】

$$\begin{aligned}
 U &= r d_1 U d_1 + r d_2 U d_2 + \cdots + r d_t U d_t \\
 &= \sum_{p=1}^t r d_p U d_p \quad (49)
 \end{aligned}$$

$$\begin{aligned}
 r d_p &= (d_1 \times d_2 \times \cdots \times d_t / d_p) \\
 &\quad / ((d_1 - d_p) \times (d_2 - d_p) \times \cdots \times (d_{p-1} - d_p) \times (d_{p+1} - d_p) \times \cdots \times (d_t - d_p)) \\
 &= \prod_{i=1}^t d_i / (d_i - d_p) \quad (50)
 \end{aligned}$$

【0 1 5 2】

逆元計算部 2 1 0 4 - j は、線形結合計算部 2 1 0 3 - j からの出力 U を受け取り、その逆元 U^{-1} を計算して、秘密分散計算部 2 1 0 5 - j へ出力する。有限体 $GF(q)$ 上の逆元は、もとの逆元をとりたい要素を $q-2$ 回乗算する次式 (51)、すなわち、

$$U^{-1} = U^{q-2} \quad \cdots (51)$$

で計算することもできる。また、ユークリッドの互除法を用いて計算することもできる。

【0 1 5 3】

秘密分散計算部 2 1 0 5 - j は、逆元計算部 2 1 0 4 - j からの出力 U^{-1} を受け取り、この出力 U^{-1} を分散して、他のメンバに秘密通信路 3 0 3 を通して配布する。第 5 の実施形態における秘密分散計算部 2 1 0 5 - j の構成は、図 16 の秘密分散計算部 1 3 0 2 - j の構成と同様なものである。第 5 の実施形態における秘密分散計算部 2 1 0 5 - j は、次式 (52) の $k'-1$ 次多項式 $f_4(x)$ を作る

【数 2 7】

$$f_4(x) = U^{-1} + R_{4,1} x + R_{4,2} x^2 + \cdots + R_{4,k'-1} x^{k'-1} \quad (52)$$

ここで、 $R_{4,1}, R_{4,2}, \cdots, R_{4,k'-1}$ は、乱数として有限体 $GF(q)$

q) 上の値を $k'-1$ 個選んだものである。

【0154】

秘密分散計算部 2105-j は、仮メンバ ID が d_p ($p=1, 2, \dots, t$) であるメンバに対して配布する分散情報 $U^{-1}d_p$ を、上記式 (52) を用いて次式 (53) のように計算する。

【数28】

$$\begin{aligned} U^{-1}d_p &= f_4(d_p) \\ &= U^{-1} + R_{4,1}(d_p) + R_{4,2}(d_p)^2 + \dots + R_{4,k'-1}(d_p)^{k'-1} \end{aligned} \quad (53)$$

【0155】

秘密分散計算部 2105-j は、自分自身に対する分散情報 $U^{-1}d_j$ は、“(2) 分散乗算部” 2106-j へ出力し、その他の分散情報 $U^{-1}d_p$ ($p=1, 2, \dots, t$ であり、 $p \neq j$ であるもの) を秘密通信路 303 を通して各メンバに配布する。

【0156】

“(2) 分散乗算部” 2106-j は、乱数生成部 2101-j からの出力と、秘密分散計算部 2105-j からの出力 $U^{-1}d_j$ を受け取り、それらを入力として、秘密通信路 303 からの情報を用いながら演算を行い、その演算結果を出力する。第5の実施形態における“(2) 分散乗算部” 2106-j の構成は、図16の“(2) 分散乗算部” 1205-j-a, 1206-j-a の構成、又は、図20の“(2) 分散乗算部” 1205-j-a, 1206-j-a の構成と同じである。第5の実施形態においては、図24(a)に示されるように、“(2) 分散乗算部” 2106-j からの出力が、仮メンバ ID が d_j である代表メンバの分散逆元計算部 1203-j-a からの出力となる。

【0157】

次に、図24(b)を用いて、代表メンバ以外のメンバ(仮メンバ ID を d_i ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの)とする)の分散逆元計算部 1203-i-a ($a=1, 2, \dots, t$) の構成を説明する。図24(b)に示さ

れるように、代表メンバ以外のメンバの分散逆元計算部 $1203-i-a$ ($a=1, 2, \dots, t$) は、乱数生成部 $2101-i$ と、“(2) 分散乗算部” $2102-i$, $2106-i$ と、公開送信部 $2107-i$ と、公開受信部 $2108-i$ とを有する。乱数生成部 $2101-i$ からの出力は、代表メンバ以外のメンバの分散逆元計算部 $1203-i-a$ へ入力される入力 Ad_i とともに、“(2) 分散乗算部” $2102-i$ へ入力される。また、乱数生成部 $2101-i$ からの出力は、“(2) 分散乗算部” $2106-i$ へも入力される。“(2) 分散乗算部” $2102-i$ からの出力は、公開送信部 $2107-i$ へ入力される。乱数生成部 $2101-i$ からの出力は、公開受信部 $2108-i$ からの出力とともに、“(2) 分散乗算部” $2106-i$ へ入力される。“(2) 分散乗算部” $2106-i$ からの出力が、代表メンバ以外のメンバの分散逆元計算部 $1203-i-a$ からの出力となる。

【0158】

図 24 (b) の乱数生成部 $2101-i$ の構成及び動作は、図 24 (a) の乱数生成部 $2101-j$ の構成及び動作と同様である。また、図 24 (b) の“(2) 分散乗算部” $2102-i$, $2106-i$ の構成及び動作は、図 24 (a) の“(2) 分散乗算部” $2102-j$, $2106-j$ の構成及び動作と同様である。

【0159】

公開送信部 $2107-i$ は、“(2) 分散乗算部” $2102-i$ からの出力を受け取り、それを、秘密通信路 303 を通して、代表メンバへ送信する。“(2) 分散乗算部” $2102-i$ からの出力を Ud_i とすると、代表メンバ以外の公開送信部 $2107-i$ ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) からの出力 Ud_i を、秘密通信路 303 を通して、代表メンバの線形結合計算部 $2103-j$ へ送信し、代表メンバの線形結合計算部 $2103-j$ は合計で $t-1$ 個の Ud_i ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) を受け取る。

【0160】

公開受信部 $2108-i$ は、秘密通信路 303 を通して、代表メンバの秘密分散計算部 $2105-j$ から $U^{-1}d_i$ を受け取り、それを“(2) 分散乗算部”

2106-iへ入力する。

【0161】

“(2) 分散乗算部” 2106-iは、乱数生成部2101-iからの出力、及び、公開受信部2108-iからの出力を受け取り、それらを入力として、秘密通信路303からの情報を用いながら演算を行い、その演算結果を出力する。第5の実施形態における“(2) 分散乗算部” 2106-iの構成は、図16の“(2) 分散乗算部” 1205-j-a, 1206-j-aの構成、又は、図20の“(2) 分散乗算部” 1205-j-a, 1206-j-aの構成と同じである。図24(b)に示されるように、“(2) 分散乗算部” 2106-iからの出力が、代表メンバ以外のメンバの分散逆元計算部1203-i-aからの出力となる。

【0162】

このように、図24の構成をとると、分散逆元計算部1203-i-aの“(2) 分散乗算部”の個数を減らすことができ、処理を簡素化することができる。

【0163】

[第5の実施形態の動作]

第5の実施形態に係る秘密再構成方法における動作は、上記第3の実施形態における動作とほぼ同じであり、図19のフローチャートとほぼ同じであるが、図19のステップS1603の動作が、異なる点を持つ。上記第3の実施形態においては、ステップS1603の計算に用いる分散逆元計算部1203-i-aは、図18のような構成により計算処理を行っていたが、第5の実施形態においては、図24のような構成により計算処理を行う。

【0164】

[第5の実施形態の効果]

以上説明したように、第5の実施形態によれば、上記第1、第2、第3の実施形態と同様に、もとの秘密情報Sを再構成するために集まったメンバの持つ分散情報を、他のメンバに公開せずに、もとの秘密情報Sを再構成することができる。したがって、各メンバが持つ分散情報を、次回の秘密再構成の際に再利用することができる。しかも、秘密再構成を行う第三者的なセンターのようなものを必

要とせずに、上記の効果を達成することができる。

【0165】

また、第5の実施形態においては、上記第3の実施形態と同様な効果を得ることができるだけでなく、上記第3の実施形態における、分散逆元計算部 $1203-j-a$ ($j=1, 2, \dots, t, a=1, 2, \dots, t$) の“(2)分散乗算部”の個数を格段に減らすことができる。

【0166】

《変形例》

[第1の実施形態の変形例]

上記第1の実施形態においては、メンバのうち、どの2人のメンバ間にも、その2人のメンバ以外には通信内容を秘密とすることができる秘密通信路が確立されていることを前提としていたが、マルチパーティ・プロトコルで用いる秘密分散法に、加算秘密分散法を用いているため、すべてを盗聴されていたとしても秘密再構成は不可能であり、秘密通信路ではなく、秘密通信路ではない(盗聴される可能性のある)通信路で通信してもよい。

【0167】

[第3の実施形態の変形例]

図25は、本発明の第3の実施形態の変形例における項計算部 $1101-j-a$ の構成を示すブロック図である。上記第3の実施形態における項計算部 $1101-j-a$ においては、図15(第3の実施形態)に示されるように、“(2)分散乗算部” $1205-j-a$ 及び“(2)分散乗算部” $1206-j-a$ は、項計算部 $1101-j-a$ へ入力される Xm'_a, j と、分散逆元計算部 $1203-j-a$ からの出力と、“(t-1)分散乗算部” $1204-j-a$ からの出力とを分散計算により掛け合わす処理を行っていたが、図15に示される“(2)分散乗算部” $1205-j-a$ 及び“(2)分散乗算部” $1206-j-a$ を、図25に示されるように、1つの“(3)分散乗算部” $1207-j-a$ に置き換えることも可能である。図25に示されるように、“(3)分散乗算部” $1207-j-a$ は、入力される3つの値の分散乗算を行う部分であり、“(t-1)分散乗算部” $1202-j-a, 1204-j-a$ と同様な構成(すなわち

、 $t-1=3$ とした構成)で実施できる。

【0168】

また、上記第3の実施形態においては、図17(第3の実施形態)に示されるように、“ $(t-1)$ 分散乗算部” $1202-j-a$ 、 $1204-j-a$ は、入力される値を、 $A_1, A_2, \dots, A_{(t-1)}$ と、 A のインデックス(下付き添え字)が小さい順に分散乗算するように構成している。しかし、分散乗算の順序は入れ替え可能なので、必ずしもこの順番(A のインデックス(下付き添え字)が小さい順)に分散乗算するように構成する必要はない。

【0169】

[第2の実施形態の変形例]

上記第2の実施形態においては、分散秘密再構成計算部 $601-j$ の秘密分散計算部 $701-j$ 、及び、秘密再構成計算部 602 が、それぞれ、 (k', t) しきい値秘密分散法による、秘密分散、及び、秘密再構成を行っている場合を説明したが、これに代えて、加算秘密分散法による、秘密分散、及び、秘密再構成を行うように構成してもよい。その場合には、秘密再構成計算部 602 において計算する上記式(22)及び(4)に代えて、次式(54)のような計算処理を行う。

【数29】

$$S = S_{m'_1} + S_{m'_2} + \dots + S_{m'_t} = \sum_{j=1}^t S_{m'_j} \quad (54)$$

また、秘密分散計算部 $701-j$ において計算する上記式(23)及び(24)に代えて、次のような計算により分散情報 $X_{m'_j, p}$ を求める。まず、乱数として有限体 $GF(q)$ の値を $t-1$ 個選んで、分散情報 $X_{m'_j, p}$ ($p=1, 2, \dots, t-1$)に割り当て、 $X_{m'_j, t}$ を次式(55)のように求める。

$$\begin{aligned} X_{m'_j, t} \\ = X_{m'_j} - (X_{m'_j, 1} + X_{m'_j, 2} + \dots + X_{m'_j, t-1}) \end{aligned} \quad (55)$$

【0170】

[第4の実施形態の変形例]

図26は、本発明の第4の実施形態の変形例における i, j 項計算部 1702-j の構成を示すブロック図である。上記第4の実施形態においては、第3の実施形態に係る秘密再構成方法における分散計算に用いる (k', t) しきい値秘密分散法のしきい値 k' の式(29)の制限を取り払うことができるので、 (k', t) しきい値秘密分散法の代わりに、加算秘密分散法を用いることができる。分散秘密再構成計算部 902-j の秘密分散計算部 1001-j における計算処理、秘密再構成計算部 903 における計算処理、及び、“(2) 分散乗算部” 1205-j-a, 1206-j-a における j, j 項計算部 1701-j における計算処理と i, j 項計算部 1702-j における構成を変更することにより、分散計算に用いる秘密分散法を加算秘密分散計算法に変更することができる。まず、分散秘密再構成計算部 902-j の秘密分散計算部 1001-j における計算処理は、式(29') 及び(30)を用いて分散情報 $X_{m', j, p}$ を求める代わりに、次のような計算処理に変更する。まず、乱数として有限体 $GF(q)$ の値を $t-1$ 個選んで、 $X_{m', j, p}$ ($p=1, 2, \dots, t-1$) に割り当て、 $X_{m', j, t}$ を次式(56)のように求める。

$$X_{m', j, t} = X_{m', j} - (X_{m', j, 1} + X_{m', j, 2} + \dots + X_{m', j, t-1}) \quad (56)$$

また、秘密再構成計算部 903 における計算処理は、式(27) 及び(28)を用いる代わりに、次式(57)のような計算処理に変更する。

【数30】

$$S = S d_1 + S d_2 + \dots + S d_t = \sum_{j=1}^t S d_j \quad (57)$$

さらに、上記第4の実施形態においては、図21 (第4の実施形態) に示されるように、“(2) 分散乗算部” 1205-j-a, 1206-j-a における j, j 項計算部 1701-j における計算処理は、“(2) 分散乗算部” 1205-j-a, 1206-j-a に入力される2つの入力 $A d_j, B d_j$ を受け取りそ

れらを乗算して、式(41)で計算される係数 r_{dj} をさらに乗算する。しかし、第4の実施形態の変形例においては、図26に示されるように、“(2)分散乗算部”1205-j-a, 1206-j-aは、係数 r_{dj} の乗算を省略するように構成されている。すなわち、第4の実施形態の変形例においては、 $A_{dj} \times B_{dj}$ を計算して出力するようにするため、図21(第4の実施形態)に示される係数乗算部1806-j-i ($i=1, 2, \dots, j-1, j+1, \dots, t$)の構成部分が削除されている。

【0171】

[第5の実施形態の変形例]

図27(a)及び(b)は、本発明の第5の実施形態の変形例における分散逆元計算部1203-j-a, 1203-i-aの構成を示すブロック図である。上記第5の実施形態においては、第3の実施形態に係る秘密再構成方法における分散計算に用いる (k', t) しきい値秘密分散法のしきい値 k' の式(29)の制限を取り払うことができる場合も考慮でき、その場合には、 (k', t) しきい値秘密分散法の代わりに、加算秘密分散法を用いることができる。上記の第4の実施形態の変更(すなわち、分散秘密再構成計算部902-jの秘密分散計算部1001-jにおける計算処理、秘密再構成計算部903における計算処理、及び、“(2)分散乗算部”1205-j-a, 1206-j-aにおけるjj項計算部1701-jにおける計算処理とij項計算部1702-jにおける構成を変更する)に加え、さらに、分散逆元計算部1203-j-a, 1203-i-aを図24(第5の実施形態)の構成から図27(第5の実施形態の変形例)のような構成に変更することにより、分散計算に用いる秘密分散法を加算秘密分散計算法に変更することができる。線形結合計算部2103-jを、“(t)加算部”2109-jに変更し、秘密分散計算部2105-j内の計算処理を変更する。秘密分散計算部2105-jの処理を変更するので、図27では、符号2110-jを付与する。“(t)加算部”2109-jは、“(2)分散乗算部”2102-jの出力結果、及び、秘密通信路303を通して他のメンバからの“(2)分散乗算部”2102-i ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの)の出力結果を受け取り、それらをすべて加算して、計算結果を逆元計算

部 2104-j へ出力する。“ (2) 分散乗算部” 2102-j の出力結果を $U d_j$ とし、秘密通信路 303 を通して他のメンバからの“ (2) 分散乗算部” 2102-i ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) の出力結果を $U d_i$ ($i=1, 2, \dots, t$ であり、 $i \neq j$ であるもの) とすると、線形結合計算部 2103-j では、式 (49) および (50) の計算処理を行って、その結果の U を出力していたが、“ (t) 加算部” 2109-j は、次式 (58) を計算し、その結果 U を逆元計算部 2104-j へ出力する。

【数 31】

$$U = U d_1 + U d_2 + \dots + U d_t = \sum_{p=1}^t U d_p. \quad (58)$$

また、秘密分散計算部 2105-j の処理を変更した秘密分散計算部 2110-j は、逆元計算部 2104-j からの出力 U^{-1} を受け取り、この出力 U^{-1} を分散して他のメンバに秘密通信路 303 を通して配布する。秘密分散計算部 2105-j は、式 (52) 及び (53) の計算処理を行って分散情報 $U^{-1} d_p$ ($p=1, 2, \dots, t$) を求めていたが、秘密分散計算部 2110-j は、次のように分散情報 $U^{-1} d_p$ ($p=1, 2, \dots, t$) を求める。まず、乱数として有限体 $GF(q)$ の値を $t-1$ 個選んで、 $U^{-1} d_p$ ($p=1, 2, \dots, t-1$) に割り当て、 $U^{-1} d_t$ を次式のように求める。

$$U^{-1} d_t = U^{-1} - (U^{-1} d_1 + U^{-1} d_2 + \dots + U^{-1} d_{t-1}) \quad (59)$$

【0172】

[他の変形例]

上記第 4 の実施形態 (及び上記第 4 の実施形態の変形例) における、“ (2) 分散乗算部” 1205-j-a, 1206-j-a において、①項計算受信部 1801-j-p ($p=1, 2, \dots, j-1$) を項計算送信部に置き換え、さらに、項計算送信部 1803-j-p ($p=j+1, j+2, \dots, t$) を項計算受信部に置き換えた構成、又は、②項計算受信部 1802-j-p ($p=1, 2, \dots$

, $j-1$) を項計算送信部に置き換え、さらに、項計算送信部 $1804-j-p$ ($p=j+1, j+2, \dots, t$) を項計算受信部に置き換えた構成、又は、③項計算受信部をすべて項計算送信部に、さらに、項計算送信部をすべて項計算受信部に置き換えた構成、などの構成でも、同様の効果を得ることができる。

【0173】

また、上記第4の実施形態（及び上記第4の実施形態の変形例）における、“（2）分散乗算部” $1205-j-a$, $1206-j-a$ において、項計算送信部 $1801-j-p$ （又は $1802-j-p$ ）と項計算受信部 $1803-p-j$ （又は $1804-p-j$ ）との間の秘密通信路 303 における情報のやり取りは、式（44）（又は式（44'））や式（46）～（48）（又は式（46'）～（48'））のように、暗号化されたような情報、すなわち、法 q のもとにおける離散対数を計算することが困難であることを利用して送りたい情報を隠蔽している情報なので、とくに秘密に通信する必要はない。式（44）（又は式（44'））においては、送りたい情報 $A d_j$ （又は $B d_j$ ）を有限体 $GF(q)$ の生成元 h のべき数として隠蔽し、式（46）～（48）（又は式（46'）～（48'））で得られる情報から得るべき必要な情報 $A d_j (a-1) - D d_{j,p}$ （又は $B d_j (a-1) - E d_{j,p}$ ）は、式（44）（又は式（44'））で用いた乱数 $r A_{p,j}$ （又は $r B_{p,j}$ ）を知らないと算出できないようになっている。したがって、上記における通信においては、秘密通信路ではない通信路（すなわち、放送型の通信路や盗聴される可能性のある通信路）で通信してもよい。

【0174】

また、上記第5の実施形態（及び上記第5の実施形態の変形例）における、分散逆元計算部 $1203-j-a$ において、代表メンバの分散逆元計算部 $1203-j-a$ における線形結合計算部 $2103-j$ （及び“（t）加算部” $2109-j$ ）、逆元計算部 $2104-j$ 、及び秘密分散計算部 $2105-j$ （ $2110-j$ ）の処理（各メンバから“（2）分散乗算部” $2102-i$ からの出力を集めて線形結合計算（加算）を行い、その結果の逆元を求め、求めた逆元をさらに秘密分散して各メンバに配布する処理）は、統合するセンターのようなものが行

い、代表メンバなしで実施する、すなわち、集まったメンバすべての分散逆元計算部 $2103-j-a$ が、図 24 (b) のような構成をとることもできる。

【0175】

また、上記第 5 の実施形態（及び上記第 5 の実施形態の変形例）における、分散逆元計算部 $1203-j-a$ において、代表メンバの線形結合計算部 $2103-j$ （及び“(t)加算部” $2109-j$ ）、と秘密通信路 303 との情報のやり取り（すなわち、代表メンバ以外のメンバの公開送信部 $2107-i$ と秘密通信路 303 との情報のやり取り）、及び、代表メンバの秘密分散計算部 $2105-j$ と秘密通信路 303 との情報のやり取り（すなわち、代表メンバ以外のメンバの公開受信部 $2108-i$ と秘密通信路 303 との情報のやり取り）は、とくに秘密に通信する必要はないので、放送型の通信路や盗聴される可能性のある通信路で通信してもよい。

【0176】

また、上記第 1～第 5 の実施形態においては「メンバ」を、演算記憶装置であるとして説明したが、本発明に係る秘密再構成方法は、複数のメンバ（人間）が分散情報を持ち寄って、複数の人間が秘密再構成処理を進めることもできる。

【0177】

さらに、上記第 1～第 5 の実施形態において、上記第 1～第 3 の実施形態の説明の効果として記述したように、集まった複数人からなるグループ全員が正当メンバ（予め秘密情報 S の分散情報を配布されたメンバ）か、そうでない人（装置）が混在するか、ということを認証するような機能があるので、その場合には、「もとの秘密情報 S」は、照合秘密情報 S（予め登録されている情報で、認証が成立するか否かを、再構成結果と照らし合わせる情報）として用いるため、必ずしもメンバに秘密な情報でなくても実現できる。

【0178】

【発明の効果】

以上説明したように、本発明によれば、各メンバが保有する分散情報又はメンバ ID を公開せずに、もとの秘密情報の再構成を行うことができるという効果が得られる。

【図面の簡単な説明】

【図 1】 (k, n) しきい値秘密分散法を実施する構成を示す図である。

【図 2】 本発明の第 1 の実施形態における秘密分散法を実施する構成を示す図である。

【図 3】 本発明の第 1 の実施形態における各メンバ及び秘密通信路を示す図である。

【図 4】 本発明の第 1 の実施形態に係る秘密再構成方法の概要を説明するための図である。

【図 5】 本発明の第 1 の実施形態に係る秘密再構成方法を実施する構成（秘密再構成システム）を示すブロック図である。

【図 6】 図 5 の分散秘密再構成計算部（分散秘密再構成装置）の構成を示すブロック図である。

【図 7】 本発明の第 1 の実施形態に係る秘密再構成方法における動作を示すフローチャートである。

【図 8】 本発明の第 2 の実施形態に係る秘密再構成方法を実施する構成（秘密再構成システム）を示すブロック図である。

【図 9】 図 8 の分散秘密再構成計算部（分散秘密再構成装置）の構成を示すブロック図である。

【図 10】 本発明の第 2 の実施形態に係る秘密再構成方法における動作を示すフローチャートである。

【図 11】 本発明の第 3 の実施形態に係る秘密再構成方法の概要を説明するための図である。

【図 12】 本発明の第 3 の実施形態に係る秘密再構成方法を実施する構成（秘密再構成システム）を示すブロック図である。

【図 13】 図 12 の分散秘密再構成計算部（分散秘密再構成装置）の構成を示すブロック図である。

【図 14】 図 13 の分散処理部の構成を示すブロック図である。

【図 15】 図 14 の項計算部の構成を示すブロック図である。

【図 16】 図 15 の“(2) 分散乗算部”の構成を示すブロック図である

【図 17】 図 15 の “ $(t-1)$ 分散乗算部” の構成を示すブロック図である。

【図 18】 図 15 の分散逆元計算部の構成を示すブロック図である。

【図 19】 本発明の第 3 の実施形態に係る秘密再構成方法における動作を示すフローチャートである。

【図 20】 本発明の第 4 の実施形態に係る秘密再構成方法で使用する “(2) 分散乗算部” の構成を示すブロック図である。

【図 21】 図 20 の i, j 項計算部の構成を示すブロック図である。

【図 22】 図 21 の項計算受信部の構成を示すブロック図である。

【図 23】 図 21 の項計算送信部の構成を示すブロック図である。

【図 24】 本発明の第 5 の実施形態に係る秘密再構成方法で使用する分散逆元計算部の構成を示すブロック図である。

【図 25】 本発明の第 3 の実施形態の変形例における項計算部の構成を示すブロック図である。

【図 26】 本発明の第 4 の実施形態の変形例における i, j 項計算部の構成を示すブロック図である。

【図 27】 本発明の第 5 の実施形態の変形例における分散逆元計算部の構成を示すブロック図である。

【符号の説明】

- 201 秘密分散計算部、
- 301 メンバの分散秘密再構成計算部（分散秘密再構成装置）、
- 301-j メンバ j の分散秘密再構成計算部、
- 302 秘密再構成装置の秘密再構成計算部、
- 303 秘密通信路、
- 401-j メンバ j の秘密分散計算部、
- 402-j メンバ j の “ (n) 加算部”、
- 601 メンバの分散秘密再構成計算部（分散秘密再構成装置）、
- 601-j メンバ ID が m_j であるメンバの分散秘密再構成計算部、

- 602 秘密再構成装置の秘密再構成計算部、
- 701-j メンバIDが m_j であるメンバの秘密分散計算部、
- 702-j メンバIDが m_j であるメンバの線形結合計算部、
- 901 仮メンバID生成部、
- 902 メンバの分散秘密再構成計算部（分散秘密再構成装置）、
- 902-j 仮メンバIDが d_j であるメンバの分散秘密再構成計算部、
- 903 秘密再構成装置の秘密再構成計算部、
- 1001-j 仮メンバIDが d_j であるメンバの秘密分散計算部、
- 1002-j 仮メンバIDが d_j であるメンバの分散処理部、
- 1101-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの項計算部、
- 1102-j 仮メンバIDが d_j であるメンバの“(t)加算部”、
- 1201-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの差分計算部、
- 1202-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの“(t-1)分散乗算部”、
- 1203-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの分散逆元計算部、
- 1204-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの“(t-1)分散乗算部”、
- 1205-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの“(2)分散乗算部”、
- 1206-j-a ($a=1, 2, \dots, t$) 仮メンバIDが d_j であるメンバの“(2)分散乗算部”、
- 1301-j 仮メンバIDが d_j であるメンバの乗算部、
- 1302-j 仮メンバIDが d_j であるメンバの秘密分散計算部、
- 1303-j 仮メンバIDが d_j であるメンバの線形結合計算部、
- 1401-1, ..., 1401-(t-2) “(2)分散乗算部”、
- 1501-1, ..., 1501-(q_b-1) “(2)分散乗算部”、

- 1502 乗算制御部、
- 1503 (q, b) 分散乗算部、
- 1701-j 仮メンバIDが d_j であるメンバの j 項計算部、
- 1702-j 仮メンバIDが d_j であるメンバの i 項計算部、
- 1703-j 仮メンバIDが d_j であるメンバの “(t) 加算部”、
- 1801-j-1, ..., 1801-j-(j-1) 仮メンバIDが d_j であるメンバの項計算受信部、
- 1802-j-1, ..., 1802-j-(j-1) 仮メンバIDが d_j であるメンバの項計算受信部、
- 1803-j-(j+1), ..., 1803-j-t 仮メンバIDが d_j であるメンバの項計算送信部、
- 1804-j-(j+1), ..., 1804-j-t 仮メンバIDが d_j であるメンバの項計算送信部、
- 1805-j-1, ..., 1805-j-(j-1), 1805-j-(j+1), ..., 1805-j-t 仮メンバIDが d_j であるメンバの加算部、
- 1806-j-1, ..., 1806-j-(j-1), 1806-j-(j+1), ..., 1806-j-t 仮メンバIDが d_j であるメンバの係数乗算部、
- 1901-j 仮メンバIDが d_j であるメンバのインデックス計算送信部、
- 1902-j 仮メンバIDが d_j であるメンバの受信復元部、
- 2001-j 仮メンバIDが d_j であるメンバの乱数生成部、
- 2002-j 仮メンバIDが d_j であるメンバの有限体要素生成部、
- 2003-j-1, ..., 2003-j-q 仮メンバIDが d_j であるメンバの乗算計算送信部、
- 2101-j 仮メンバIDが d_j であるメンバの乱数生成部、
- 2102-j 仮メンバIDが d_j であるメンバの “(2) 分散乗算部”、
- 2103-j 仮メンバIDが d_j であるメンバの線形結合計算部、
- 2104-j 仮メンバIDが d_j であるメンバの逆元計算部、
- 2105-j 仮メンバIDが d_j であるメンバの秘密分散計算部、
- 2106-j 仮メンバIDが d_j であるメンバの “(2) 分散乗算部”、

2107-i 仮メンバIDが d_j であるメンバの公開送信部、

2108-i 仮メンバIDが d_j であるメンバの公開受信部、

S もとの秘密情報、

m_1, m_2, \dots, m_n メンバID、

m'_1, m'_2, \dots, m'_t 集まったメンバのメンバID、

d_1, d_2, \dots, d_t 仮メンバID、

X_{m_j} メンバIDが m_j であるメンバに配布される分散情報、

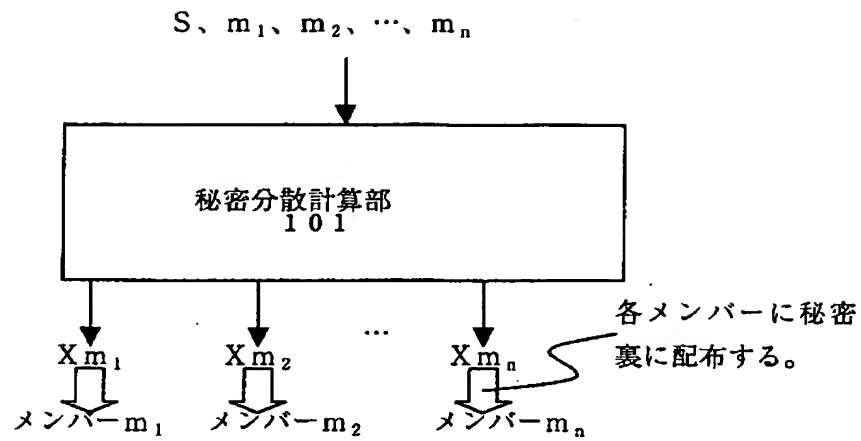
$X_{m_j, p}$ メンバIDが m_j であるメンバからメンバIDが m_p であるメンバ p に対して配布する分散情報、

S_j メンバ j が分散再構成した分散情報。

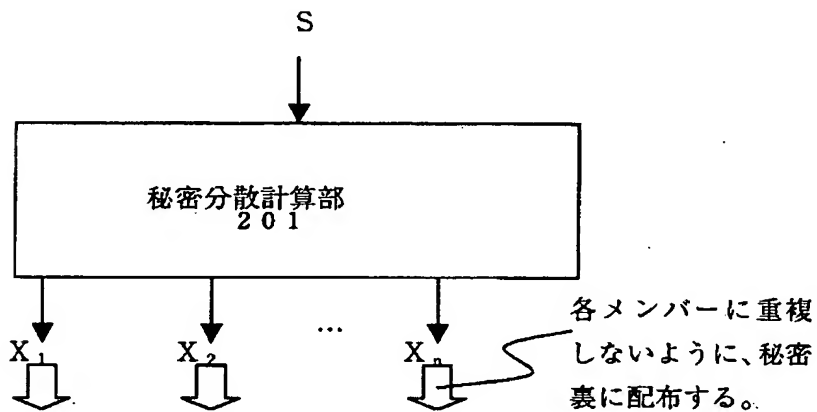
【書類名】

図面

【図 1】

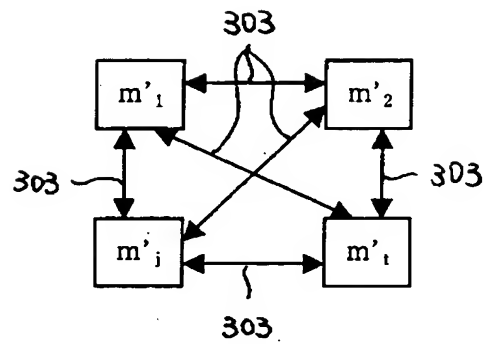
 (k, n) しきい値秘密分散法

【図 2】



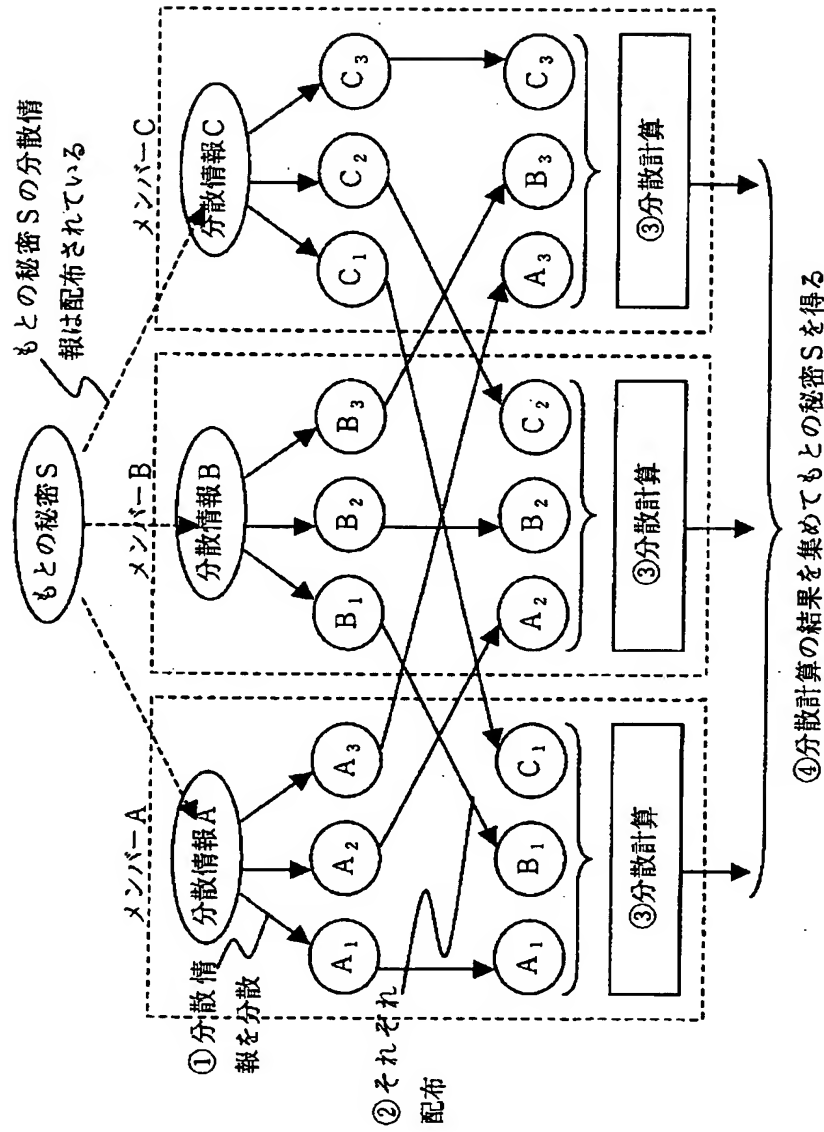
第 1 の実施形態における秘密分散

【図 3】



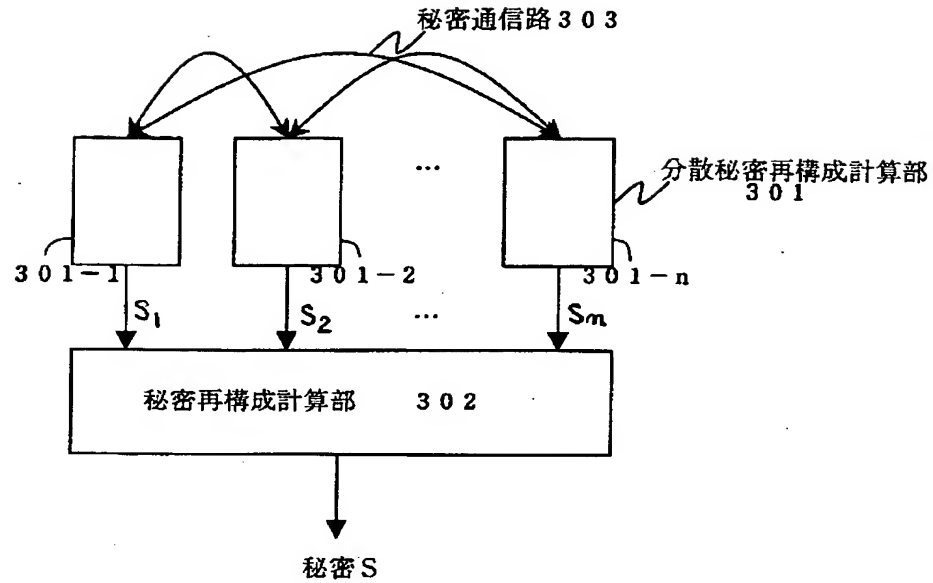
第 1 の実施形態における各メンバ及び秘密通信路

【図 4】



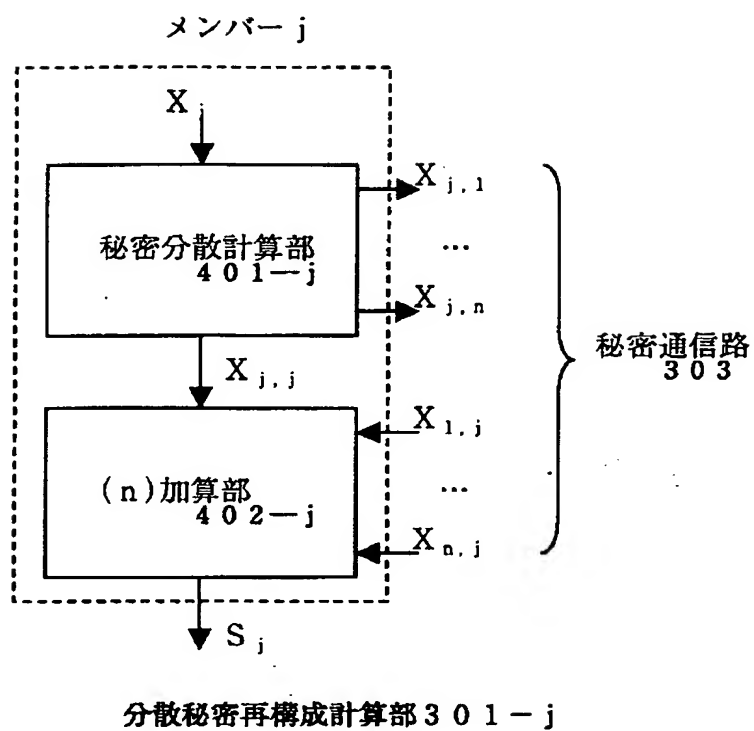
第 1 の実施形態の秘密再構成方法の概要

【図 5】

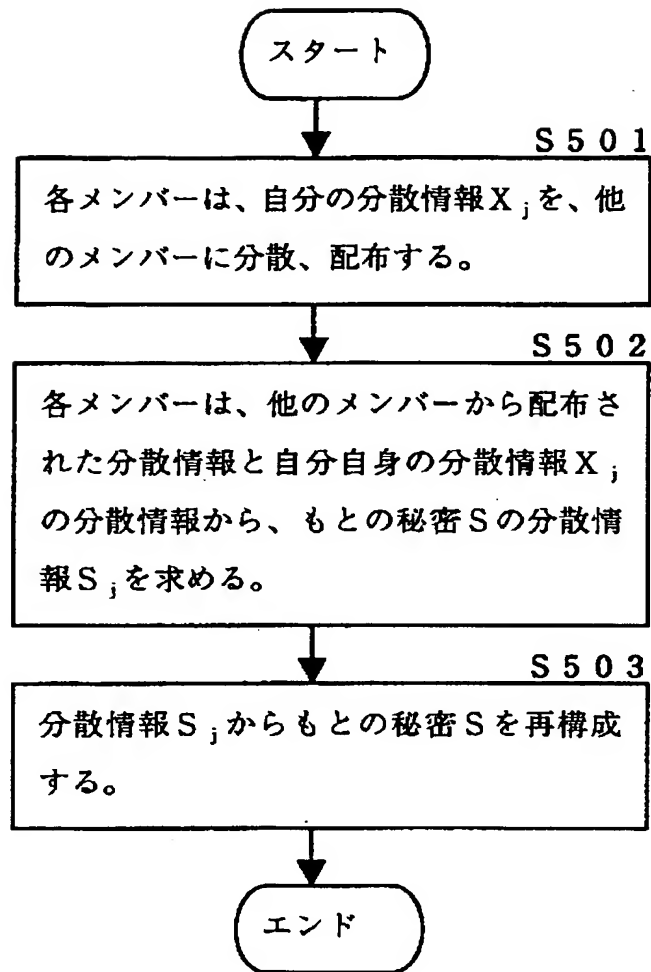


第 1 の実施形態の秘密再構成

【図 6】

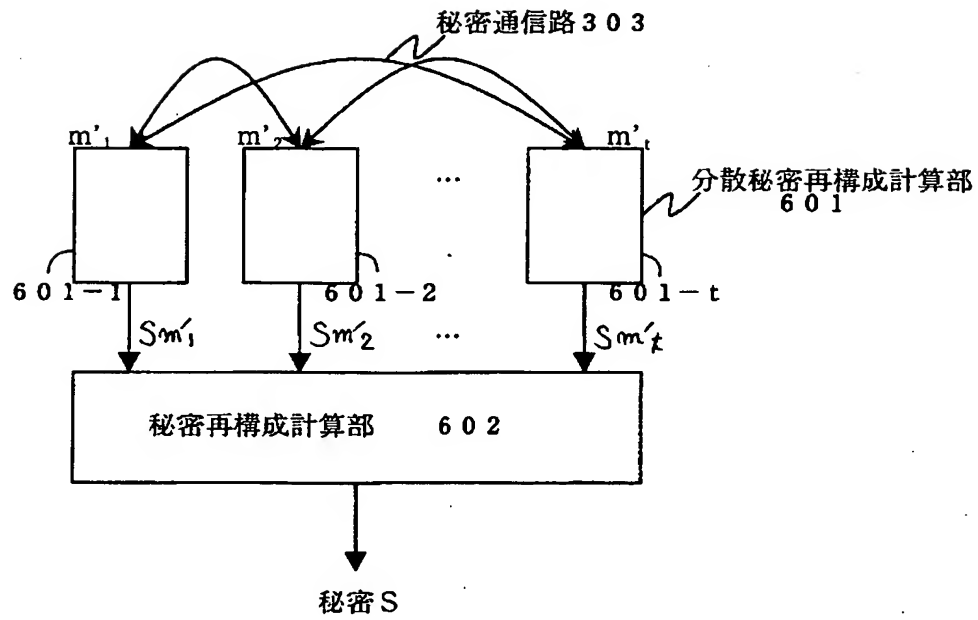


【図 7】



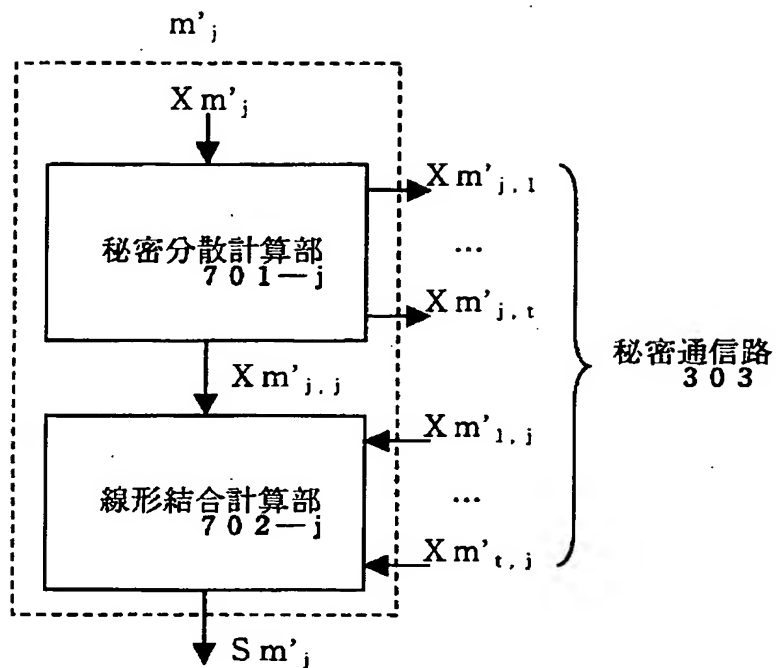
第 1 の実施形態の動作

【図 8】



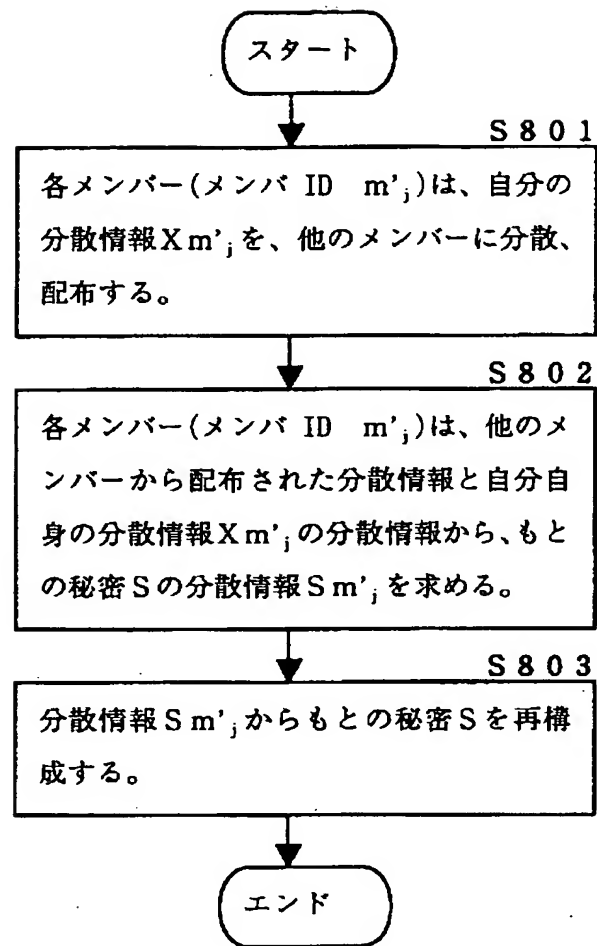
第 2 の実施形態の秘密再構成

【図 9】



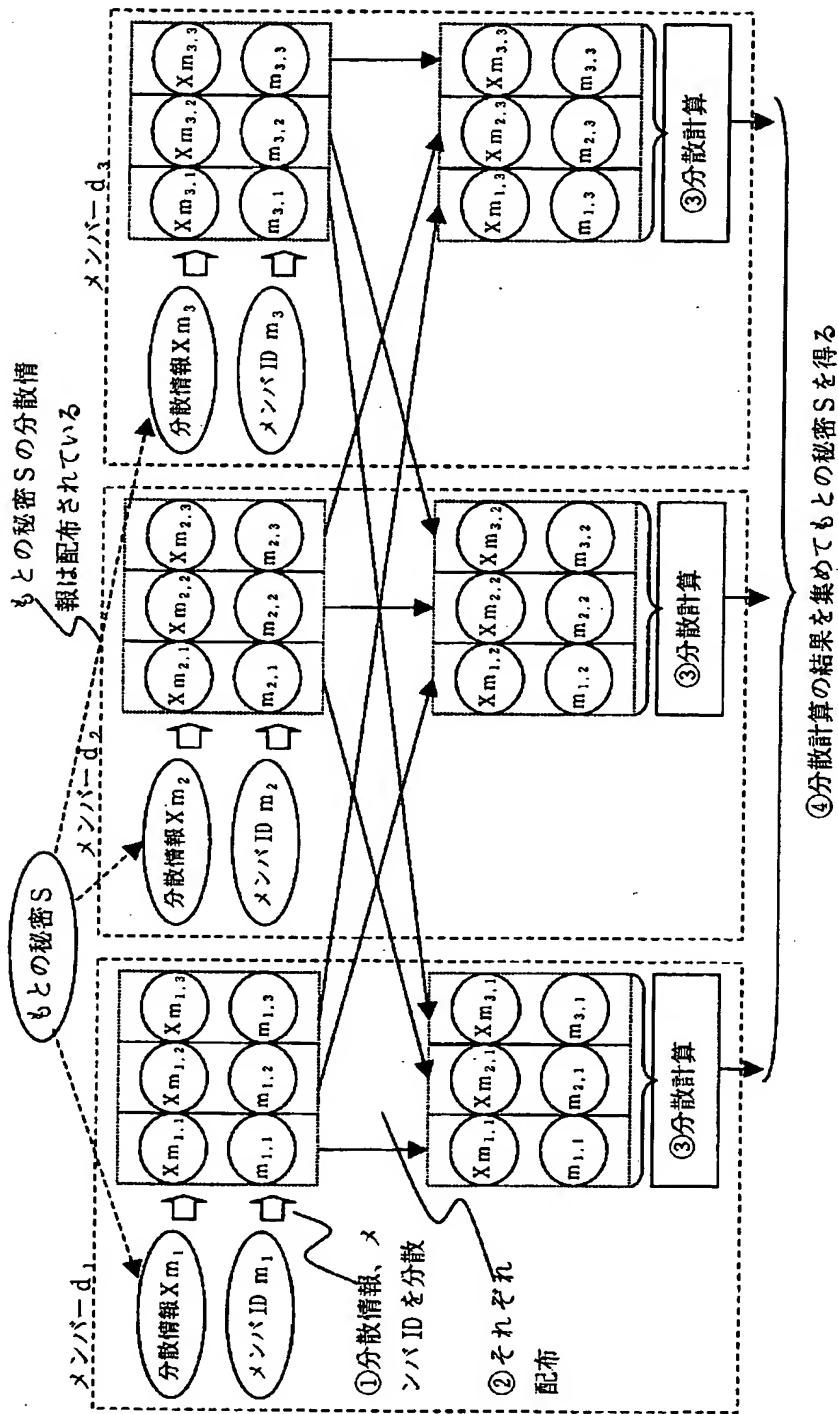
分散秘密再構成計算部 601-j

【図 10】



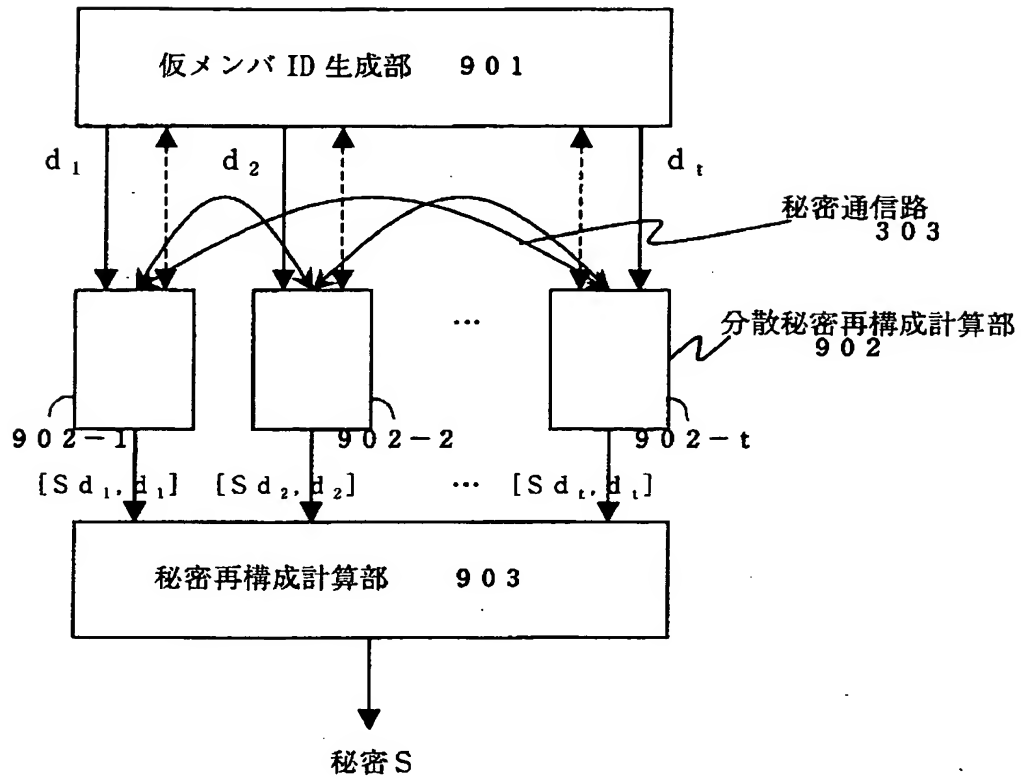
第 2 の実施形態の動作

【図 11】



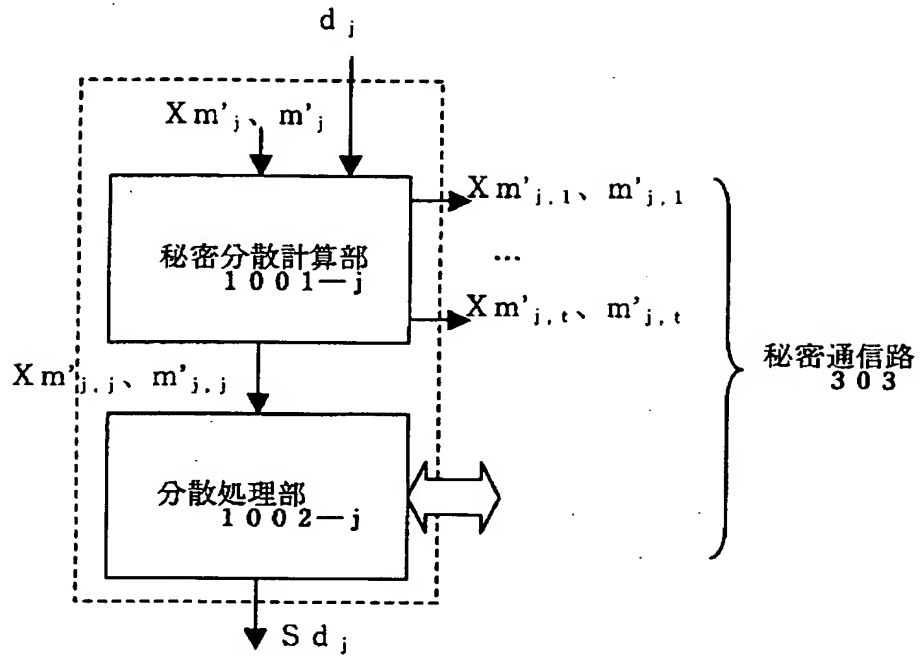
第 3 の実施形態の秘密再構成方法の概要

【図 12】



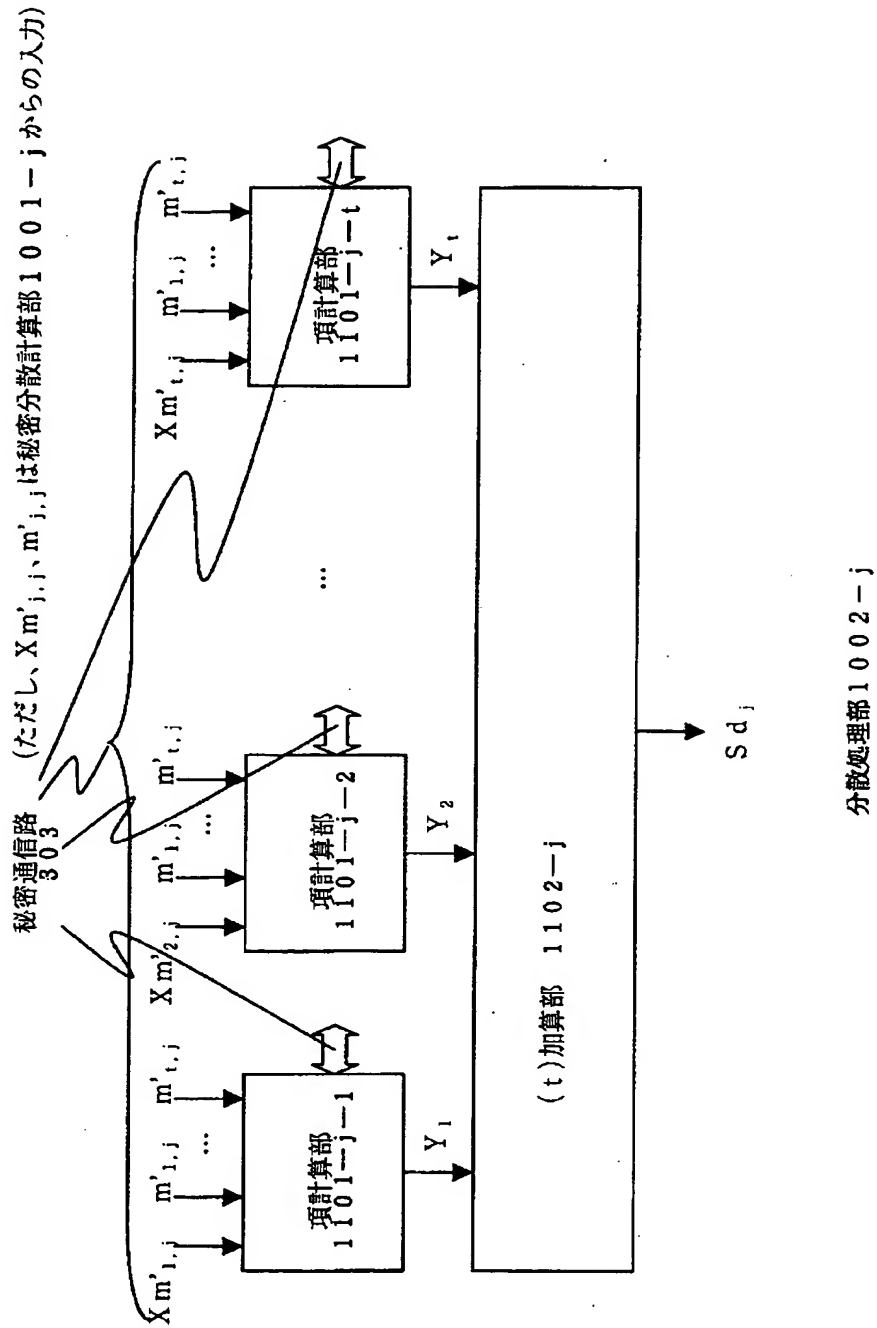
第 3 の実施形態の秘密再構成

【図 13】

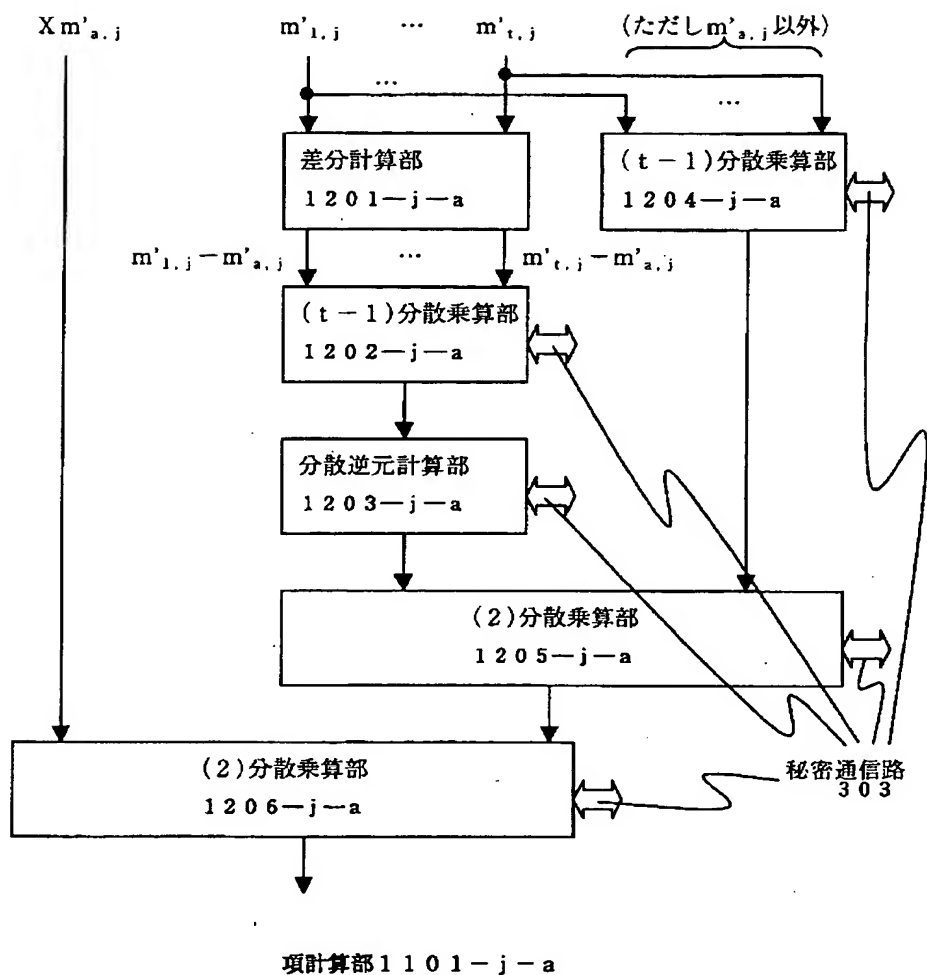


分散秘密再構成計算部 902-j

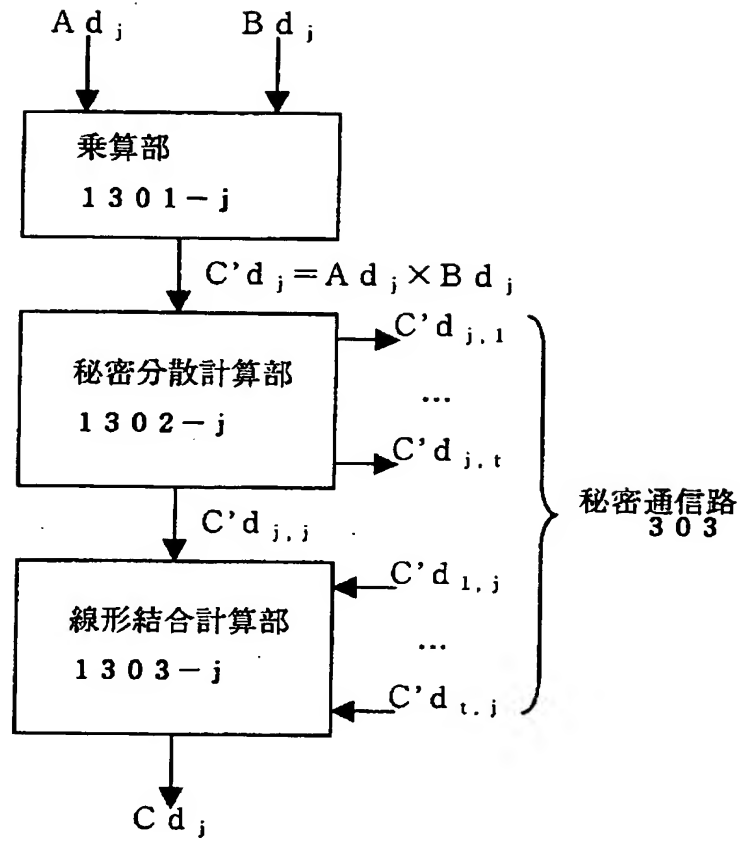
【図 14】



【図 15】

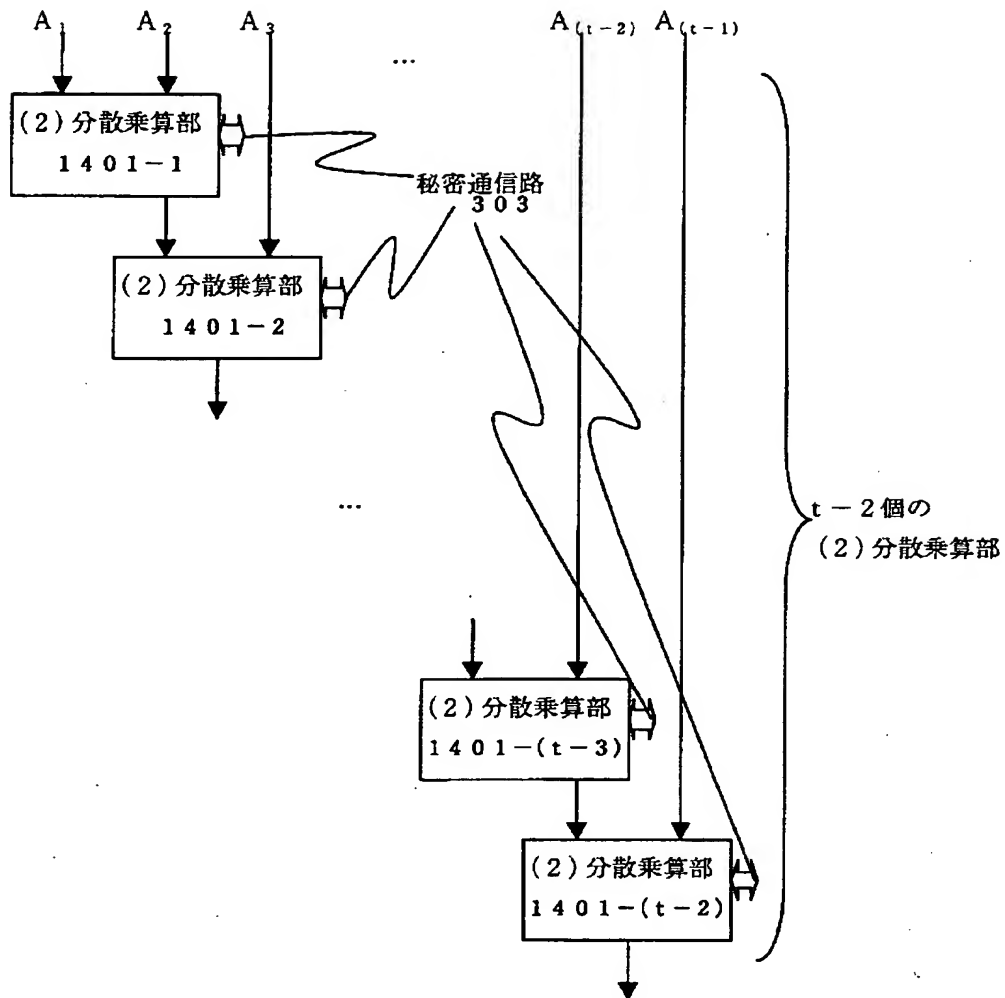


【図 16】



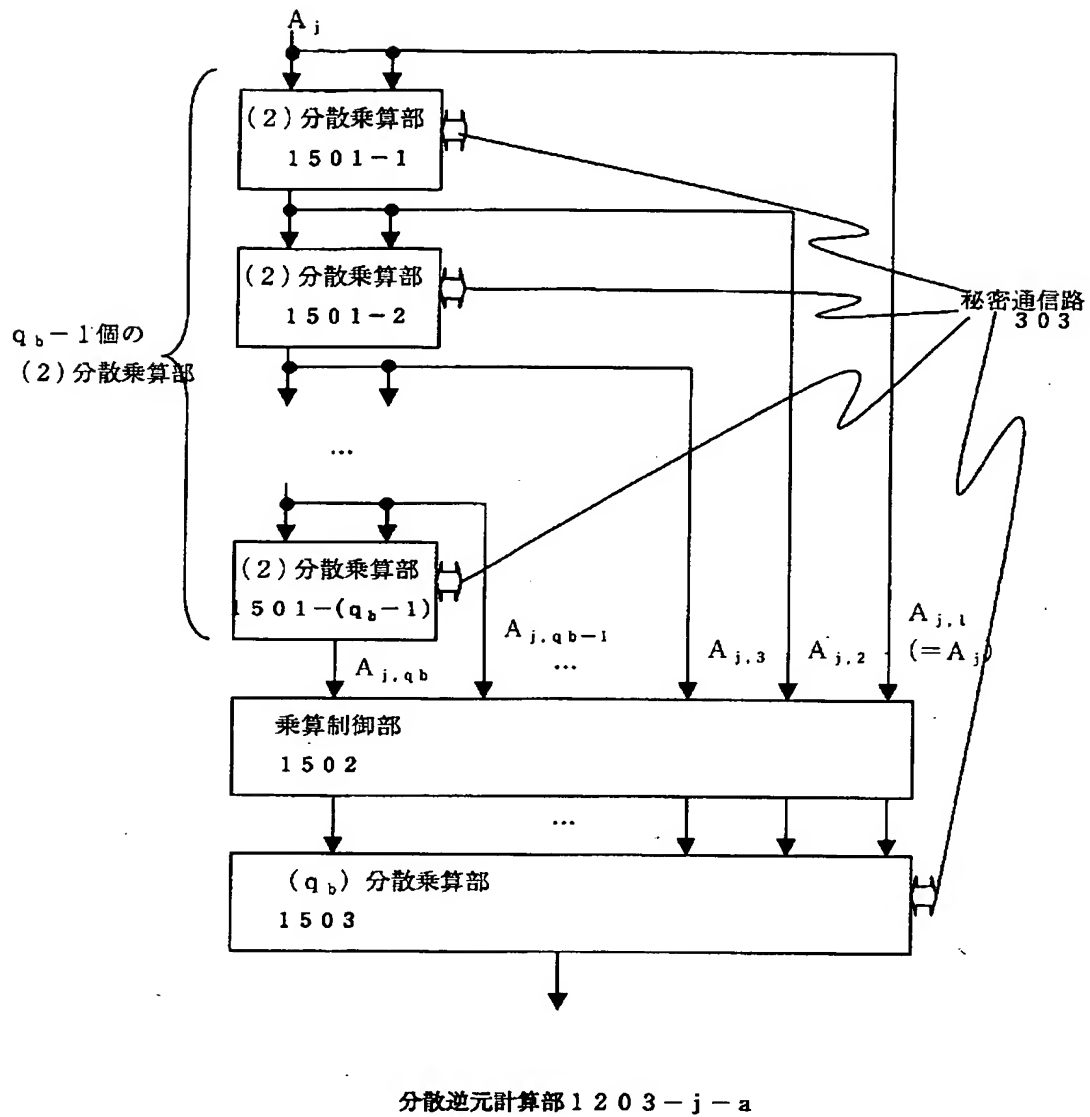
(2)分散乗算部 1205-j-a、1206-j-a

【図 17】

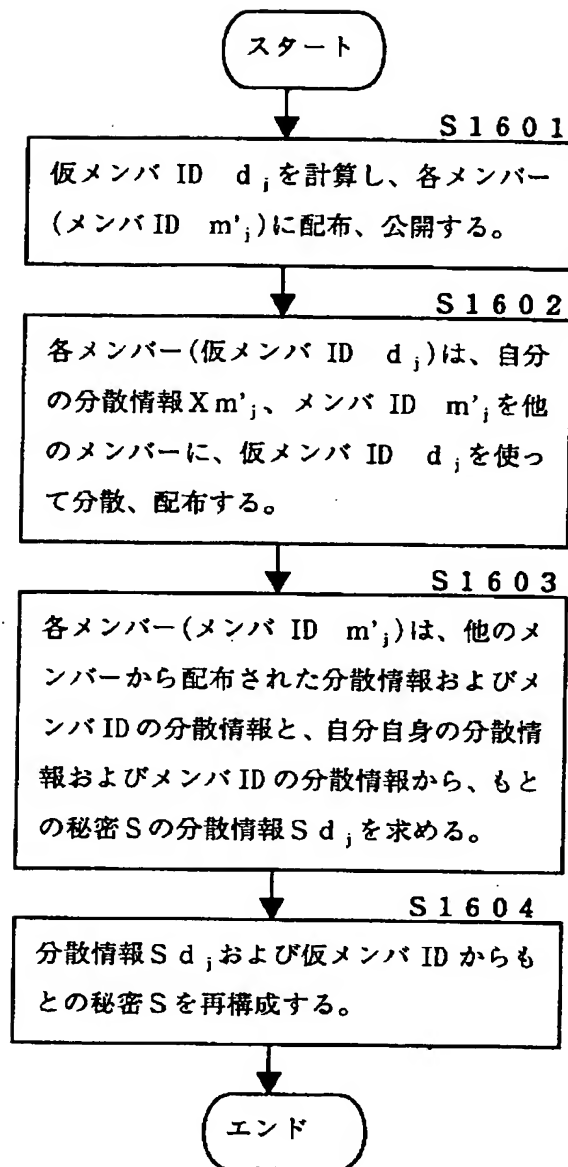


(t-1) 分散乗算部 1202-j-a、1204-j-a

【図 18】

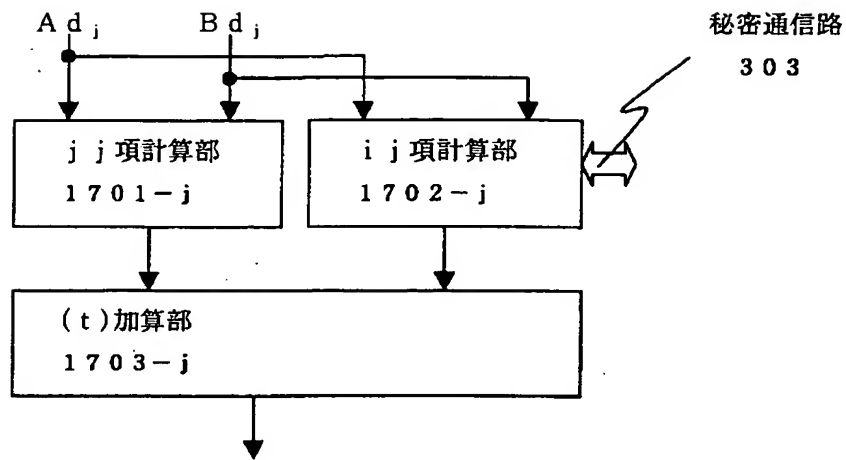


【図 19】



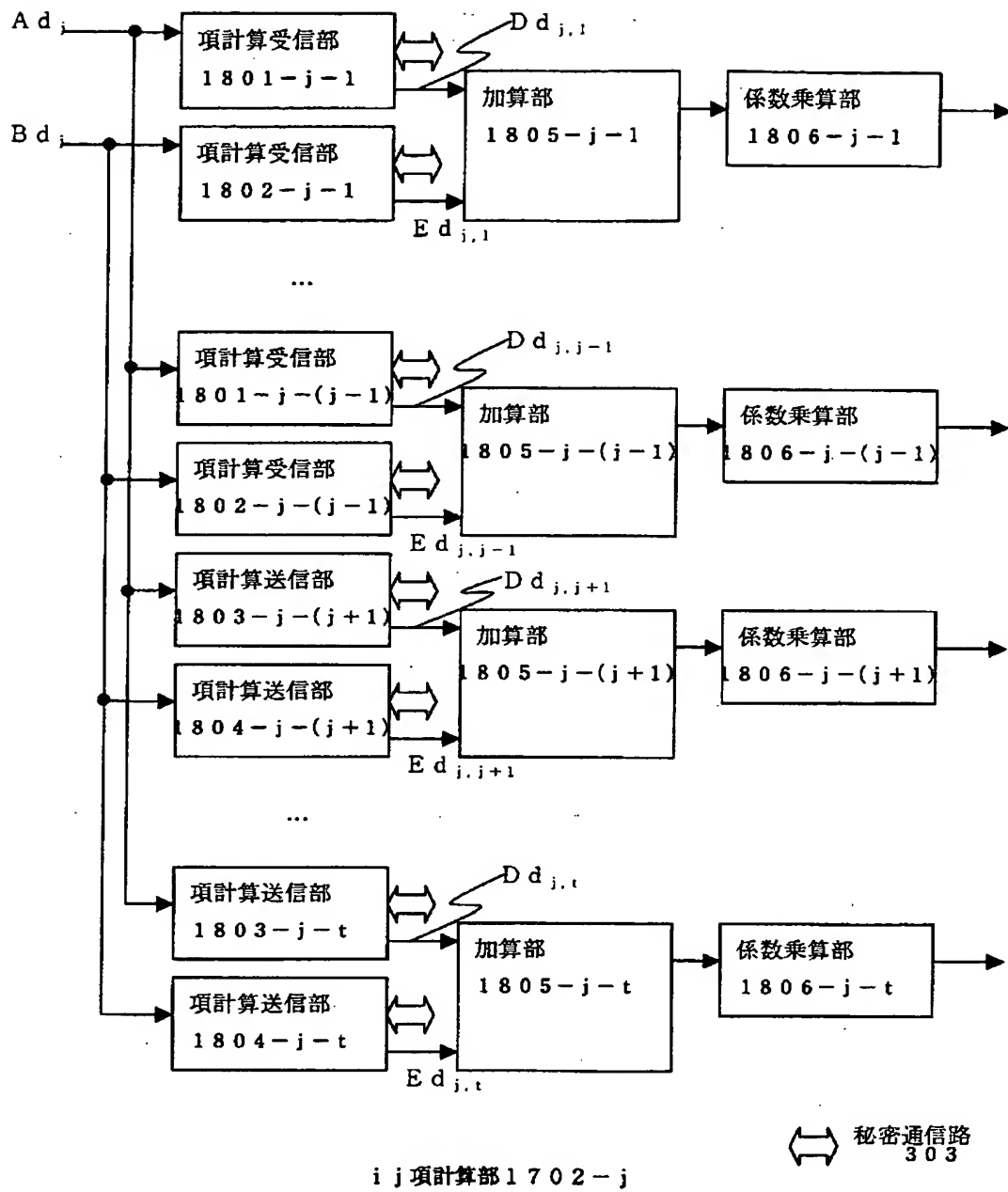
第 3 の実施形態の動作

【図 20】

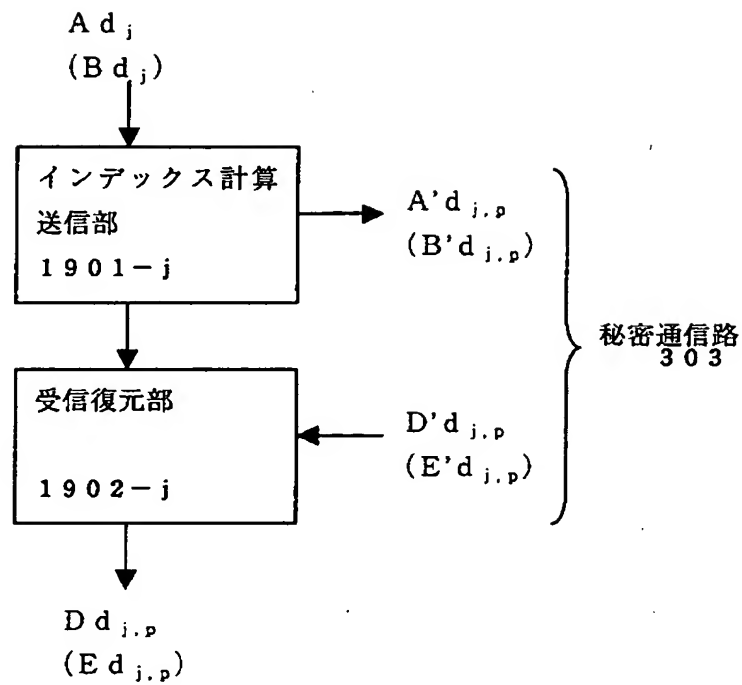


(2)分散乗算部 1205-j-a、1206-j-a (第4の実施形態)

【図 21】

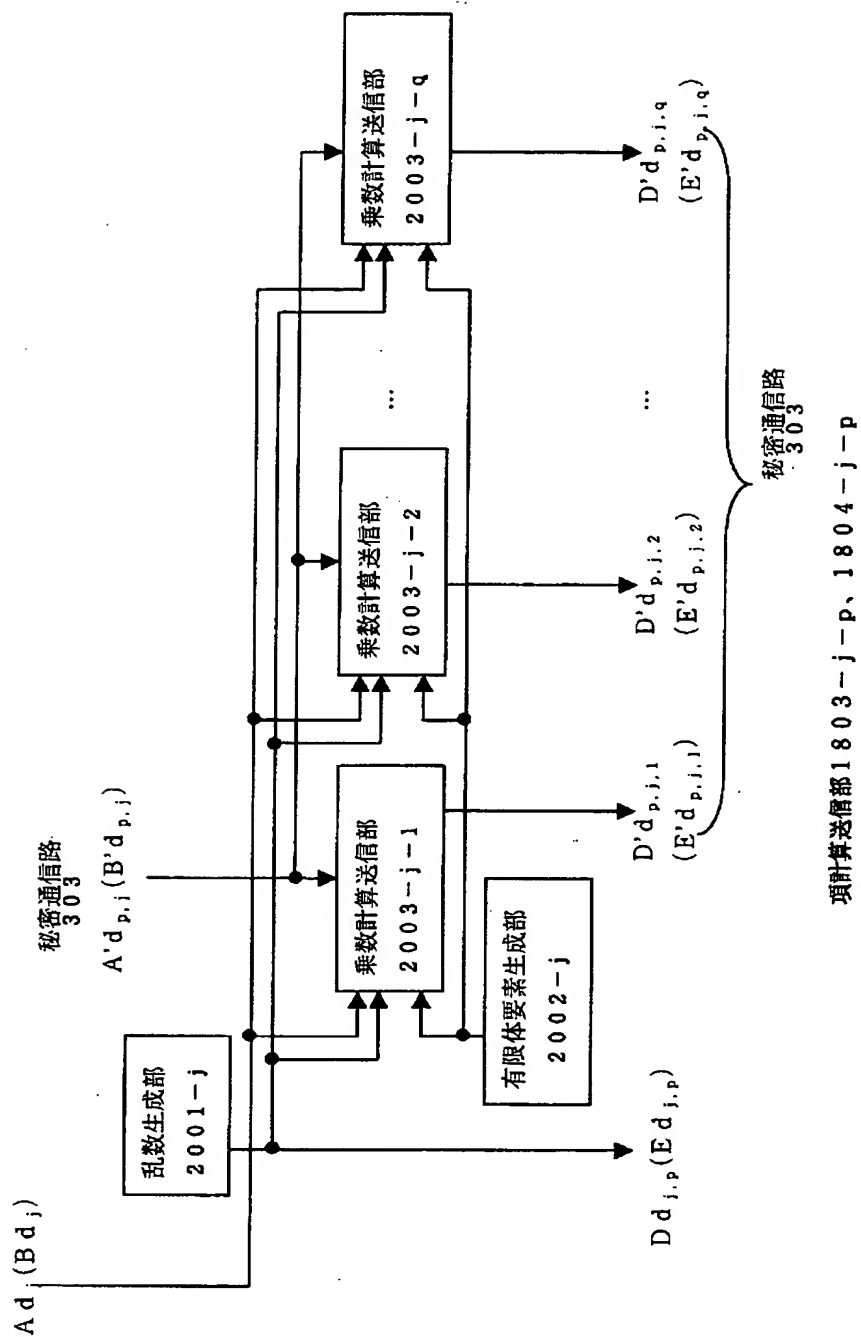


【図 22】

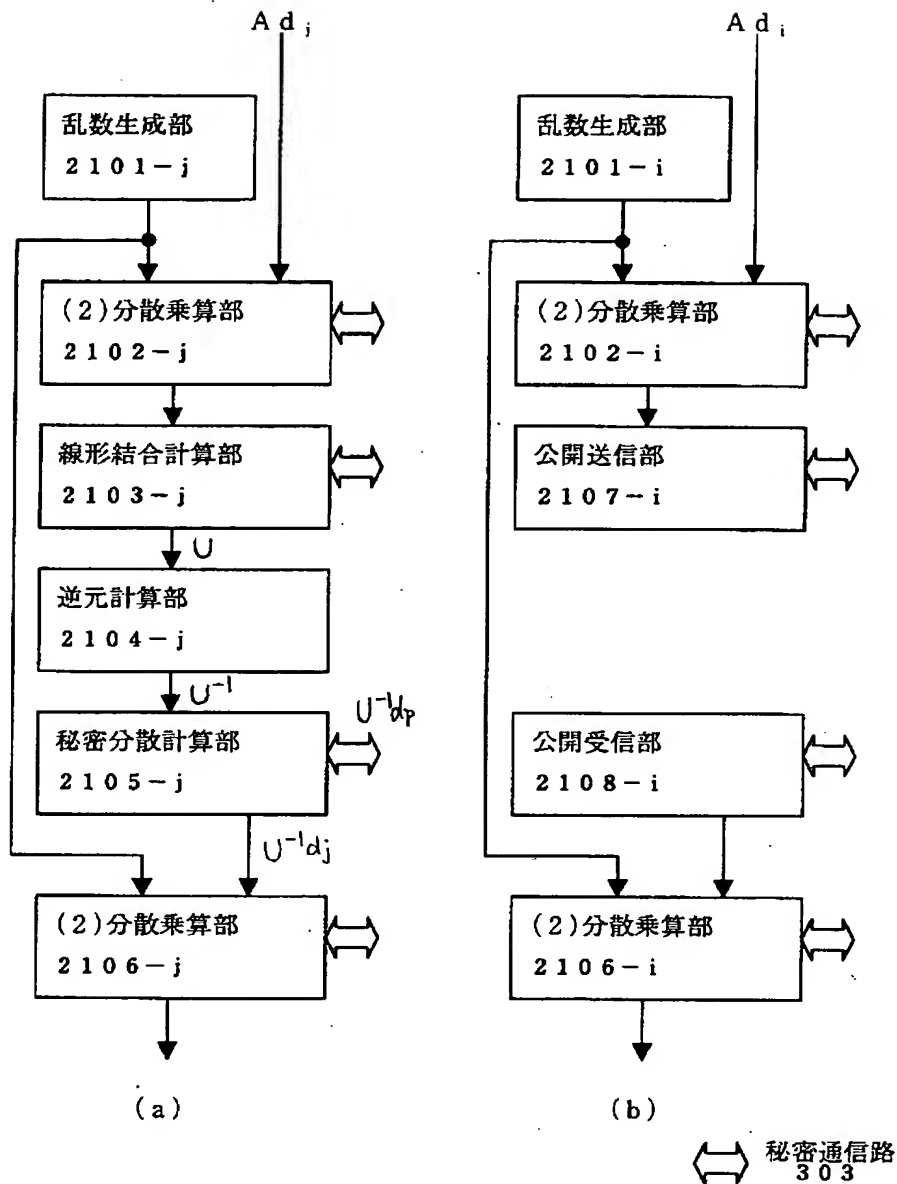


項計算受信部 1801-j-p、1802-j-p

【図 23】

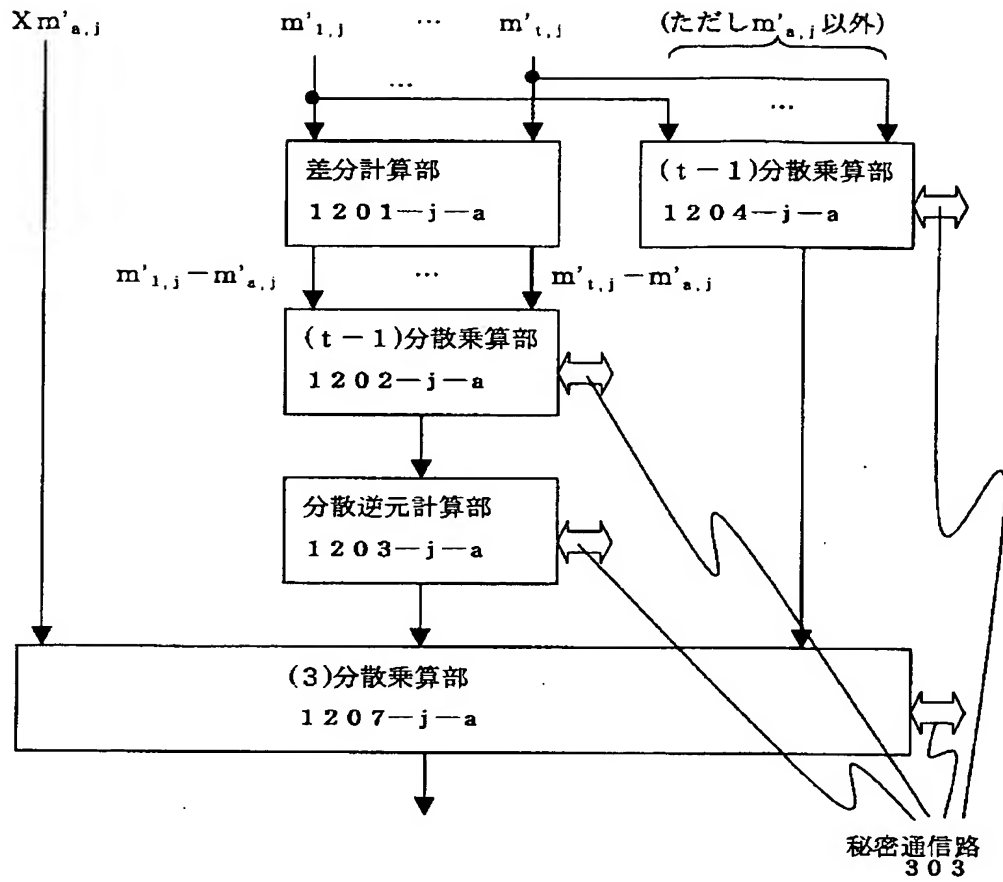


【図 24】



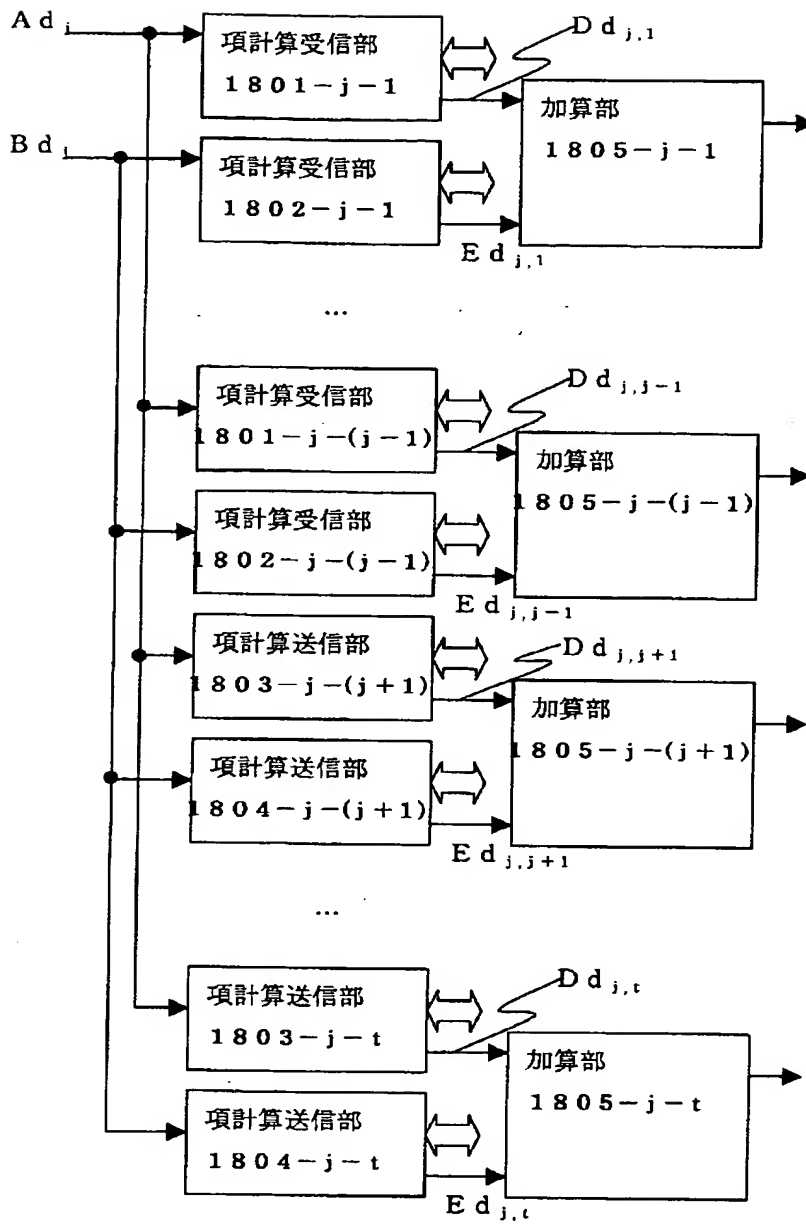
分散逆元計算部 1203-j-a (第5の実施形態)

【図 25】



項計算部 1101-j-a (変形例)

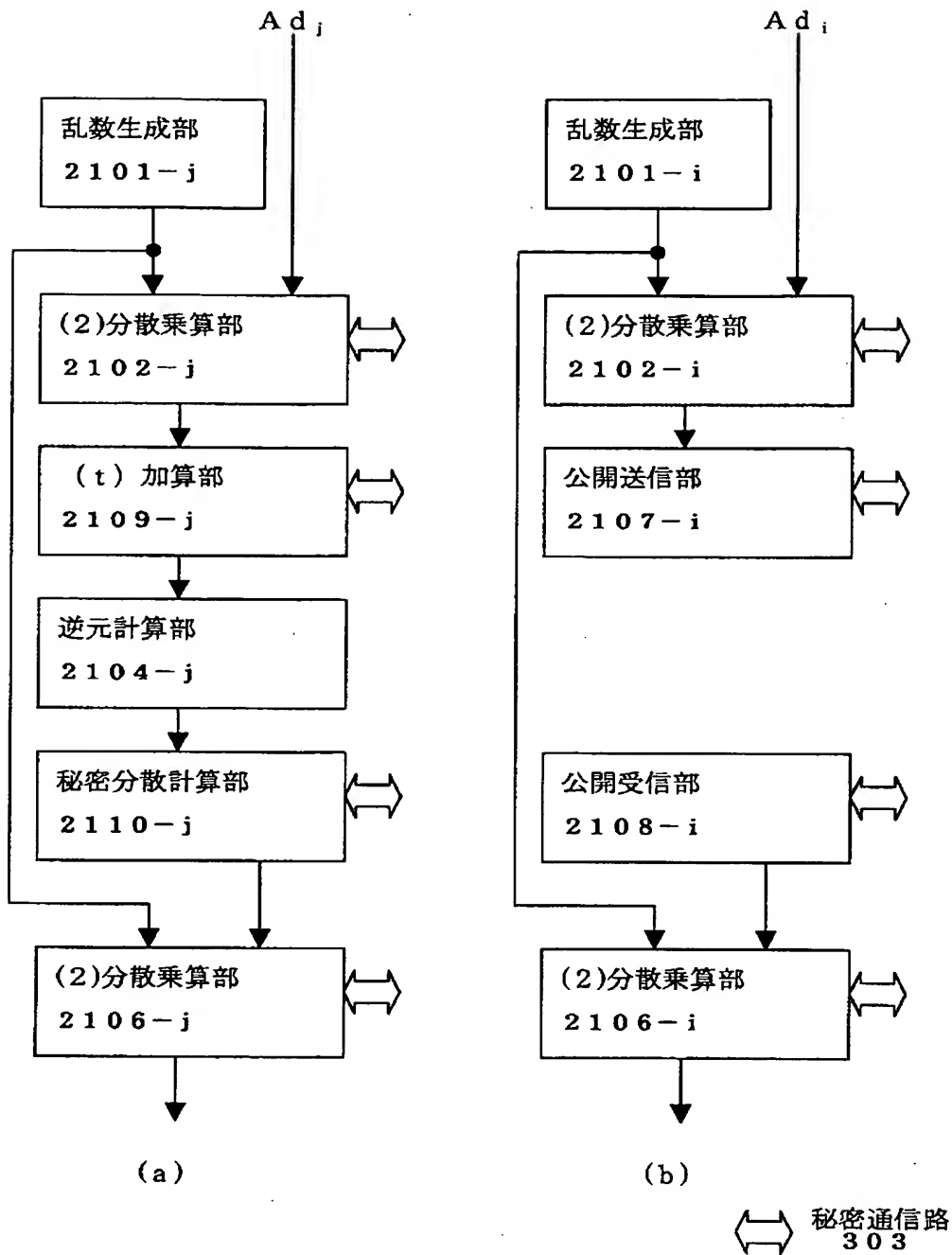
【図 26】



秘密通信路

i j 項計算部 1702-j (変形例)

【図 27】



分散逆元計算部 1203-j-a (変形例)

【書類名】 要約書

【要約】

【課題】 各メンバが保有する分散情報を公開せずに、もとの秘密情報の再構成を行う秘密再構成方法、分散秘密再構成装置、秘密再構成システムを提供する。

【解決手段】 秘密再構成方法は、ある秘密情報 S から第 1 の分散情報 X_i ($i = 1, 2, \dots, n$) を生成し各メンバに配布している場合に、 t ($2 \leq t \leq n$) 人のメンバが集まって、もとの秘密情報 S を再構成する秘密再構成方法である。再構成に際しては、集まった各メンバにおいて、各自のメンバが持つ第 1 の分散情報 X_i を秘密としたまま、秘密分散法を用いて第 1 の分散情報 X_i を分散して第 2 の分散情報 $X_{j,i}$ ($j = 1, 2, \dots, n$) として他の各メンバに対して配布し、他のメンバから第 2 の分散情報 $X_{j,i}$ を受け取ることにより、もとの秘密情報 S を再構成するための中間計算結果 S_i を、分散計算により算出し、各メンバにおける中間計算結果 S_i から、もとの秘密情報 S を再構成する。

【選択図】 図 5

・特願 2003-067834

出 願 人 履 歴 情 報

識別番号

[000000295]

1. 変更年月日

1990年 8月22日

[変更理由]

新規登録

住 所

東京都港区虎ノ門1丁目7番12号

氏 名

沖電気工業株式会社